ELECTRONIC PRIVACY INFORMATION CENTER

EX PARTE OR LATE FILED

epic.org

Via U.S. Mail

May 3, 2002

ORIGINAL

1718 Connecticut Ave NW
Suite 200
Washington DC 20009
USA
+1 202 483 1140 [tel]
+1 202 483 1248 [fax]
www.epic.org

Ms. Magalie Roman Salas
Secretary
Federal Communications Commission
445 12th Street SW, Room TWB-204
Washington, DC 20554

RE: *Ex Parte* – Telecommunications Carriers' Use Of Customer Proprietary Network Information And Other Customer Information
CC Docket No 96-115

Dear Ms. Roman Salas:

As referenced in my letter of April 31, 2001, the enclosed documents supplement the documentary record in the above-referenced docket.

If you have any questions or concerns, please feel free to contact me at (202) 483-1140 ext. 112.

Sincerely,

Mikal Condon

Mikal J. Condon
Staff Counsel

cc: Marcy Greene, Esq. (via personal delivery)
Bill Dever, Esq. (without enclosure) (via U.S. mail)

epic.org

May 3, 2002

Ms. Magalie Roman Salas
Secretary
Federal Communications Commission
445 12th Street SW, Room TWB-204
Washington, DC 20554

1718 Connecticut Ave NW
Suite 200
Washington DC 20009
USA
+1 202 483 1140 [tel]
+1 202 483 1248 [fax]
www.epic.org

RE: *Ex Parte* – Telecommunications Carriers' Use Of Customer Proprietary Network Information And Other Customer Information
CC Docket No 96-115

Dear Ms. Roman Salas:

On April 30, 2002, Megan Gray, Esq. and I of the Electronic Privacy Information Center met with Marcy Greene, Esq. and Bill Dever, Esq. of the Competitive Policy Division of the Wireline Competition Bureau regarding the Commission's Second Further Notice of Proposed Rulemaking (Notice) in the above reference docket.

In this meeting, EPIC elaborated on why the privacy protection of customer "approval," as mandated by Section 222(c)(1), can only effectively be obtained through an opt-out approach to telecommunications carriers' use of customer proprietary network information (CPNI). We emphasized that an opt-out approach has demonstrably failed to provide informed consent.

As discussed in that meeting, EPIC will be supplementing the documentary record. These documents will be faxed separately.

A copy of this electronically filed notice is being submitted to the Secretary of the FCC in accordance with Section 1.1206 of the Commission rules. If there are any questions, please feel free to contact me.

Sincerely,

Mikal J. Condon

Mikal J. Condon
Staff Counsel

cc: Marcy Greene, Esq. (via fax (202) 418-1413)
Bill Dever, Esq.

Finance

COMMENTARY: WHEN BANKS ACT LIKE BROKERS, WHO REGULATES?

The abusive atmosphere at the securities division of NationsBank Corp. in the early 1990s was shocking even for veteran stockbrokers. Working at the bank's branches, several recalled, they were told to hawk NationsBank's investment products to bank customers without explaining that they were brokers, not bankers. When elderly customers came in to roll over jumbo certificates of deposit, bank tellers got a cut of the commissions for turning them over to brokers who sold them NationsSecurities' risky closed-end bond funds instead.

When NationsSecurities' brokers complained to their bosses, say ex-employees, they got the brush-off. According to the ex-brokers, Charles King, then executive vice-president of NationsSecurities, told them to keep selling; sales targets would be raised, he warned, not lowered. Meanwhile, the main fund they were hawking, Nations Term Trust 2003, lost 35% of its value in just seven months, in part because of investments in risky derivatives. They later regained the losses.

When BUSINESS WEEK first reported the troubles at NationsSecurities nearly four years ago, NationsBank, based in Charlotte, N.C., denied any improper sales practices and said it had no problem with procedures at NationsSecurities. But on May 4, the bank forked over $6.75 million to settle administrative proceedings without admitting or denying allegations of misleading sales practices brought by banking and securities regulators. King and two other bank officials personally were fined and suspended as brokers for up to six months. King could not be reached for comment. The bank says the settlement "puts the issue behind us."

Those fines come on top of more than $60 million NationsBank has paid to settle class actions in two customer and administrative complaints in Florida, Texas, and South Carolina.

But let's not cheer regulators for their aggressive enforcement just yet. The bank got off easy. Our balkanized regulatory system's rules would have made it difficult to hold personally responsible top bank executives such as CEO

UNITED STATES OF AMERICA
Before the
SECURITIES AND EXCHANGE COMMISSION

SECURITIES ACT OF 1933
Release No. 7532 / May 4, 1998

SECURITIES EXCHANGE ACT OF 1934
Release No. 39947 / May 4, 1998

ADMINISTRATIVE PROCEEDING
File No. 3- 9596

In the Matter of :
: ORDER INSTITUTING CEASE-AND-
NATIONSSECURITIES : DESIST PROCEEDINGS PURSUANT TO
and : SECTION 8A OF THE SECURITIES
NATIONSBANK, N.A. : ACT OF 1933 AND SECTIONS:15(b)(4) AND
: 21C OF THE SECURITIES EXCHANGE ACT OF
Respondents. : 1934 AND FINDINGS AND
: ORDER OF THE COMMISSION

:
:

I.

The Commission deems it appropriate and in the public interest to initiate public administrative proceedings pursuant to Section 8A of the Securities Act of 1933 ("Securities Act") and Sections 15(b)(4) and 21C of the Securities Exchange Act of 1934 ("Exchange Act") against NationsSecurities and NationsBank, N.A. ("NationsBank") (collectively, the "respondents").

In anticipation of the institution of these proceedings, the respondents have submitted Offers of Settlement ("Offers") for the purpose of disposing of the issues raised by these proceedings. Solely for the purpose of these proceedings and any other proceeding brought by or on behalf of the Commission or to which the Commission is a party, and prior to a hearing pursuant to the Commission's Rules of Practice, the respondents, without admitting or denying the matters set forth herein, consent to the issuance of this Order Instituting Cease-and-Desist Proceedings Pursuant to Section 8A of the Securities Act of 1933 and Sections 15(b)(4) and 21C of the Securities Exchange Act of 1934 and Findings and Order of the Commission ("Order") as set forth below.

The Commission has determined that it is appropriate and in the public interest to accept the respondents' Offers and accordingly is issuing this Order.

II.

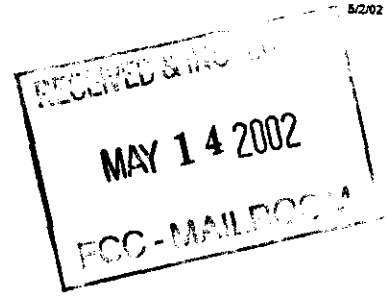
FACTS

On the basis of this Order and NationsSecurities' and NationsBank's Offers of Settlement, the Commission finds[1] the following:

A. Respondents

NationsSecurities, a broker-dealer registered with the Commission, commenced operations on June 7, 1993, as a joint venture between operating subsidiaries of Dean Witter and NationsBank. Dean Witter's interest in the joint venture was purchased by a subsidiary of NationsBank on November 15, 1994.

NationsBank is an indirect subsidiary of NationsBank Corporation, a North Carolina corporation which has common stock registered with the Commission pursuant to Section 12(b) of the Exchange Act



NationsSecurities' management asked NationsBank of North Carolina, N.A. to design term trust products for NationsSecurities to offer to NationsBank customers. Following this request, portfolio managers at NationsBank created Nations Government Income Term Trust 2003 ("Term Trust 2003") and, later, Nations Government Income Term Trust 2004 ("Term Trust 2004") (collectively the "Term Trusts").

The Term Trusts were designed to generate, at least in their early years, competitive yields of between 1% and 1.5% above the yield on then-issued ten year Treasury notes, and to return their full $10 per share investment at the end of their ten year term. While the Term Trusts were comprised to some extent of traditional government securities, they also included less conservative components intended to help the funds achieve their income and yield goals. The Term Trusts had the ability to invest up to 40% of their net assets in inverse floaters and to use leverage of up to 33% of their net assets, to hedge against interest rate changes and to produce the premium yield. The leverage created by these components helped make the net asset values of the Term Trusts highly sensitive to changes in interest rates. [4]

NationsSecurities made Term Trusts 2003 and 2004 its first two "focus products." Wholesalers made presentations to NationsSecurities registered representatives on how to sell the Term Trusts, and monetary incentive programs were offered to registered representatives for sales of the Term Trusts. Between August and September 1993, NationsSecurities offered the Term Trust 2003; Term Trust 2004 was offered during January and February 1994.

3.The Sales Effort For The Term Trusts

NationsBank arranged for the Term Trusts to retain Stephens, the underwriter, as its master selling agent for the sale of the Term Trusts. NationsSecurities and Stephens were responsible for generating sales of these products. Four Stephens wholesalers made presentations to the NationsSecurities registered representatives who would be selling the Term Trusts, and Stephens assigned one of its vice presidents to supervise the wholesalers. The Sales Manager assumed significant involvement in the promotion of the Term Trusts. The Sales Manager, who was involved with the Term Trusts at an early stage, provided information and sales instruction to the NationsSecurities registered representatives and educated the Stephens wholesalers concerning the products. He also coordinated the promotional efforts of the Stephens wholesalers, and had significant input in how they performed their assignments.

NationsSecurities considered the Term Trusts sales effort a success: 16,682,139 shares of Term Trust 2003 were sold during the August and September 1993 offering period for total proceeds of $166,821,390. The shares were sold primarily by NationsSecurities registered representatives, which resulted in approximately $9,175,176.40 in sales concessions and fees that were shared by NationsSecurities and Stephens. Term Trust 2004 sold 13,748,939 shares during its offering period of January and February 1994 for total proceeds of $137,489,390. Term Trust 2004 sales generated approximately $7,561,916.40 in combined sales concessions and fees for NationsSecurities and Stephens. NationsBank was entitled to receive advisory and administrative fees for its participation with the Term Trusts. NationsBank has waived its advisory and administrative fees during the period from June 1995 through the present.

Shares of both Term Trusts were sold to investors for $10 per share in the initial public offerings ("IPO"). In 1994, significant interest rate increases adversely affected the net asset value of the Term Trusts' portfolios. By November 18, 1994, Term Trust 2003 had fallen to a low of $6 per share on the NYSE, primarily due to rising interest rates. Similarly, by November 14, 1994, Term Trust 2004 had fallen to a low of $6.50 per share. This drop in share value generated a large number of complaints from investors who complained that they had not been informed by their registered representatives, at the time they purchased the Term Trusts, that their investments were sensitive

were contrary to the guidance provided by the OCC which states that bank employees could only receive payment in exchange for referrals that are nominal in nature and not based on a completed sale.

2.Materially False And Misleading Statements

a.The Risks Of The Term Trusts Were Not Disclosed

NationsSecurities' and NationsBank's marketing efforts involved the dissemination of materially false and misleading statements in connection with the offer and sale of the Term Trusts. As a result, some of the registered representatives gave customers misleading information concerning such material facts as the composition of the Term Trusts, risks associated with the Term Trusts, and the stability of the Term Trusts as an investment. This misinformation was disseminated to NationsSecurities registered representatives during conference calls and meetings, as well as through the circulation of several sales scripts. [9]

NationsSecurities' sales representatives attended presentations during which they were told that the Term Trusts were safe investments because they were backed by the U.S. Government. Representatives were also falsely told that NationsBank would not allow its customers to lose principal. On a number of occasions, the Sales Manager held up a picture of the Term Trust 2003 brochure which contained a picture of the U.S. Capitol Building on it, and said that NationsBank stated that "if the Capitol is standing in 10 years, these people [investors] will get their money back." Some of the registered representatives were also told that the Term Trusts were as safe as CDs or were "guaranteed" to return an investor's $10 share price at the end of the ten year term.

The Sales Manager misrepresented the suitability of the Term Trusts during his sales presentations, stating they were suitable for everyone. These misrepresentations were repeated by some NationsSecurities branch managers and wholesalers. For example, registered representatives were told that the Term Trusts were safe, had low risk and low volatility, and were suitable for everyone, even elderly people. The Sales Manager also understated the risks of an investment in the Term Trusts, and rather than discuss the use of derivatives and leverage in the Trusts, he emphasized the high returns that investors could expect. Some registered representatives were told that the 2003 was a "plain vanilla" product.

The Stephens wholesalers made similar misrepresentations in several of their presentations to the NationsSecurities registered representatives. During at least two presentations, registered representatives were told that the Term Trust 2004 was "guaranteed" to return $10 in ten years. One wholesaler also instructed registered representatives to work around the question regarding FDIC insurance by not answering it directly and focusing instead on the issue of safety. In addition, the Term Trust was described misleadingly as an "alternative to a certificate of deposit for conservative bank customers."

NationsSecurities also disseminated information concerning the Term Trusts through sales scripts designed for registered representatives to use during "call nights." [10] One script emphasized the safety and predictability of the Term Trust but failed to disclose any risks. [11] A document that a NationsSecurities senior manager ("Senior Manager") distributed to the firm's branch managers recommended that registered representatives use the phrase "SPR" which stood for "safety, predictability and return" in reference to the Term Trusts. A sales script used at call nights in the Metro District of Columbia region stated that the Term Trust 2003 provided "certainty in an uncertain world -- return of $10 in 10 years."

b.Other Misrepresentations Concerning The Term Trusts

representatives that "[a] letter about [NationsSecurities] will often have more credibility with a bank customer if it goes out on NationsBank letterhead under a bank employee's signature." On some occasions, NationsBank employees sent out letters introducing the NationsSecurities registered representative in their branch by name and explaining some of the products the registered representative could offer them. Contrary to written bank policies, at times NationsBank employees sent these letters on letterhead containing the "Member FDIC" legend. NationsBank employees also occasionally mailed letters to bank customers using NationsSecurities letterhead, despite the fact that NationsSecurities registered representatives were instructed to prevent such an occurrence.

NationsSecurities' and NationsBank's advertising materials also contributed to the blurring. Early NationsSecurities posters that appeared in NationsBank banking centers contained the slogans, "Invest in Tomorrow Where You Bank Today," and "Introducing the Investment Firm You Can Bank On." The NASD told NationsSecurities to remove these posters due to the possibility of confusion, and NationsSecurities complied.

Finally, NationsSecurities trained its registered representatives to use the terminology commonly used by bank employees to downplay the differences between the two organizations. The Sales Manager, the wholesalers, and the Branch Manager encouraged registered representatives to avoid using brokerage firm terms. For example, some NationsSecurities registered representatives were trained to refer to shares in the Term Trusts as "accounts" or "accounts at the bank" rather than as mutual funds or securities. Some registered representatives also were taught to refer to NationsSecurities as the "investment division" of NationsBank and to tell NationsBank customers they were calling "from the bank." NationsSecurities registered representatives also were called "Investment Officers" rather than brokers or account executives. [13]

The Sales Manager favored the use of bank language because it would make a bank customer more comfortable, although he also conceded that he would not have instructed registered representatives at a stand-alone non-bank broker-dealer office to use the same terminology. Indeed, the Sales Manager dictated a sales script to a Tampa registered representative that told the representative to use blurring language, including such statements as "[I'm] [c]alling from NationsBank branch. I'm with NationsSecurities which is the bank's investment division . . . [D]o you have a relationship w/us here at NationsBank? . . . If we had a higher return than [Bank X] or any other bank in town[,] wh[at] type of asset would you have available over the next 3 weeks to place in this account?" According to the Sales Manager, avoiding investment "lingo" would be helpful to bank customers because they would find bank terminology more familiar and thus "less alarming" than investment terminology.

This blurring conduct, taken together, created an atmosphere in which a bank customer could conclude that the NationsSecurities registered representative was a bank employee and that, therefore, the product purchased was a bank product. Indeed, numerous investor complaints reflect the belief that they were buying a bank product or that the NationsSecurities registered representative was a bank employee.

FOOTNOTES

[1]: The findings herein are solely for the purpose of these proceedings and are not binding on any other person in this or any other proceeding.

[2]: This Order also applies to all other federally chartered banks affiliated with NationsBank, N.A., including NationsBank of Texas, N.A., NationsBank of Tennessee, N.A., and NationsBank of Kentucky, N.A.

[3]: Simultaneous with the issuance of this Order, the National Association of Securities Dealers Regulation, Inc. ("NASDR") issued a settled order in the following matter: Letter

of its trading on the NYSE. The script did not disclose that the price obtainable on the NYSE might well be less than the original purchase price.

[12]: A registered representative stated that a NationsSecurities manager had told him that people would think he was a bank employee because "if it walks like a duck and quacks like a duck, then it's probably a duck."

[13]: In December 1993, the NASD directed NationsSecurities to stop using this title for their registered representatives because of the possibility of customer confusion.

F.NationsSecurities' Failure To Supervise

NationsSecurities adopted a "hub and spoke" organizational structure and a supervisory and compliance system based on Dean Witter's policies and procedures. Under the hub and spoke structure, supervisors worked in hubs while the registered representatives worked in spokes located in many of the over 2,000 individual NationsBank banking centers scattered throughout the surrounding area. The branch managers, who were located in the hubs, supervised anywhere from fifteen to thirty registered representatives who were located in the surrounding spokes. [14] The spokes were frequently located in remote areas miles from the hub. These features of the hub and spoke system increased the need for more centralized and focused supervisory and compliance systems. Although the supervisory system, as implemented at NationsSecurities, may have been suitable for a traditional brokerage firm, it was not, under these circumstances, reasonably designed to detect and prevent improper sales practices.

1.Blurring

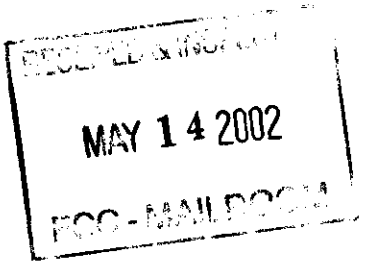
NationsSecurities' practices and procedures to prevent blurring were inadequate to prevent investor confusion between bank products and the Term Trusts. Although the firm's manuals identified such appropriate disclosures as products "are not FDIC insured" and "are not obligations of the bank," NationsSecurities did not always adequately differentiate its employees from NationsBank employees and the Term Trusts from insured bank products. The requirement of annual visits by branch managers to spoke offices was inadequate to assure that effective anti-blurring measures were in place.

2.Improper Sales Practices

NationsSecurities' supervisory and compliance system was inadequate to provide timely detection or prevention of improper sales practices. NationsSecurities required only annual visits by its branch managers to each spoke office. This decentralized and infrequent system of review failed to deter adequately improper sales practices by some individual representatives. The use of two hundred inexperienced representatives in spoke offices increased the potential for improper sales practices. There also was no effective mechanism in place to supervise the interactions of the registered representatives with the Sales Manager and the wholesalers.

3.Suitability

NationsSecurities' supervisory and compliance systems were inadequate to prevent unsuitable sales. In many cases, NationsSecurities failed to collect sufficient data on customer risk tolerance and investment horizon or failed to properly utilize the information that had been received. Although management was aware of the suitability risks of price volatile proprietary closed-end funds, such as the Term Trusts, the broker-dealer failed to create controls to ensure suitability. In addition, NationsSecurities failed to maintain in a readily



branch managers failed adequately to question registered representatives about suitability.

Failure to supervise violations frequently follow upon the existence of "red flags" that should have put the broker-dealer on notice of underlying problems. In this case, however, the absence of such warnings reflects the inability of NationsSecurities to detect the unsuitable trades in the Term Trusts that resulted from improper sales practices. The Commission has recognized that the inadequacy of a broker-dealer's supervisory system may preclude the appearance of red flags:

While the presence of 'red flags' warning of possible irregularities may often be an aggravating factor, the absence of such warning signs is not a defense where the gravamen of the supervisory deficiency is a failure to have reasonable procedures. [17]

C. NationsSecurities' Failure Reasonably To Supervise The Registered Representatives Extended To Their Interactions With The Sales Manager And The Wholesalers

NationsSecurities had responsibility for ensuring that its registered representatives were properly trained and informed. NationsSecurities failed to take appropriate steps to ensure that the presentations made by the Sales Manager and the wholesalers did not contain materially false and misleading information. NationsSecurities could have taken such steps because the conduct at issue occurred at NationsSecurities' offices, at meetings sponsored by NationsSecurities, or on telephone conference calls conducted for the benefit of NationsSecurities registered representatives. All of these meetings and calls were arranged by NationsSecurities employees. Furthermore, when such meetings occurred, some NationsSecurities' branch managers did not take adequate steps to limit the conduct of the Sales Manager and the wholesalers as they interacted with NationsSecurities employees.

D. Violations By NationsBank

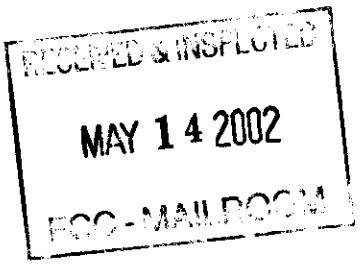
NationsBank employees engaged in activities that blurred the distinction between the bank and the brokerage firm and their respective products. Although certain of these practices were not, per se, illegal, taken together and in conjunction with the false and misleading sales practices described herein, they contributed to customer confusion and unsuitable securities purchases. The referral fee program helped to blur the distinction between the bank and the brokerage by encouraging bank employees to discuss specific securities products with bank customers. In some instances, NationsBank allowed NationsSecurities' registered representatives to sit at desks in bank lobbies without signs or other demarcations distinguishing them from the bank; mailed marketing materials in envelopes that appeared to enclose bank notices; directed bank employees to send letters to customers introducing the registered representatives; permitted bank employees to make improper sales presentations to customers; and provided registered representatives with bank-account information to use in making sales calls.

In addition, the Sales Manager and the wholesalers he trained made materially false and misleading statements to the NationsSecurities registered representatives regarding the Term Trusts and encouraged the representatives to engage in blurring and misleading sales practices. Accordingly, NationsBank contributed to and therefore was a cause of NationsSecurities' violations of Section 17(a)(2) and (3) of the Securities Act.

E. Conclusion

With the marked increase in the involvement of financial institutions in securities activities, there is a corresponding increase in the risk that some investors may be unaware of the distinction between bank products and securities products. Brokerage and financial institutions must be acutely sensitive to the potential for customer confusion inherent in the operation of a broker-dealer on the premises of a bank. Because the very nature of a brokerage firm operating in a bank environment poses a risk of investor confusion, broker-dealers in this situation

more traditionally organized firms." The Commission also has emphasized that the need for central control increases as branch offices become more numerous, dispersed and distant. See, e.g., In re Dickinson, Sec. Exch. Act Rel. No. 36338, 1995 SEC Lexis 2665 (Oct. 5, 1995) (citing Shearson, Hamill & Co., Sec. Exch. Act Rel. No. 7743, 42 SEC 811, 843 (1965)); In re Grayson, Sec. Exch. Act Rel. No. 33298, 1993 SEC Lexis 3403 at *8 (Dec. 8, 1993) at *10 (citing In re Parodi, Sec. Exch. Act Rel. No. 27299, 44 SEC Docket 1337, 1346 (Sept. 27, 1989)).



[16]: See In re GKN Securities Corp., Sec. Exch. Act Rel. No. 38173, 1997 SEC Lexis 111 at *8 (Jan. 15, 1997) (the Commission stated that "there is a particularly strong and obvious need" for adequate supervisory and compliance systems where a broker-dealer has hired relatively inexperienced sales representatives); accord Grayson at *10 (citation omitted).

[17]: In re Giordano, Sec. Exch. Act Rel. No. 36742, 1996 SEC Lexis 71 at *12 (Jan. 19, 1996) (citing In re Chambers, Sec. Exch. Act Rel. No. 27963, 46 SEC Docket 200 (Apr. 30, 1990); In re Blinder, Robinson & Co., Sec. Exch. Act Rel. No. 19057, 26 SEC Docket 238 (Sept. 17, 1982). The Commission reiterated this position in Royal Alliance, 1997 SEC Lexis 113 at *14 (Jan. 15, 1997).

[18]: Since the activities described herein, NationsSecurities was acquired by NationsBanc Investments, Inc. The findings and sanctions contained herein apply to NationsBanc Investments, Inc. and to any future successor entity.

FTC Lowers Boom on Net Porn Scammers

By Lori Enos
E-Commerce Times
September 08, 2000
http://www.ecommercetimes.com/perl/story/4233.html

FTC Chairman Robert Pitofsky

Continuing its crackdown on porn sites that illegally bill customers, the U.S. Federal Trade Commission (FTC) announced Thursday that it has won a $37.5 million (US$) judgment against an adult Web site operation that was billing customers for X-rated Internet visits they had not made and services they did not order.

A federal judge in California issued the order last month after finding that Malibu, California residents Kenneth Taves, Teresa Callei Taves, Dennis Rappaport and their businesses had illegally billed more than 700,000 customers for over $40 million. The three owned J.K. Publications, Inc.; MJD Service Corp.; Herbal Care, Inc.; and Discreet Bill, Inc.

The defendants operated 14 different adult Web sites from June 1997 through early January 1999, when the FTC initially filed the case and a federal judge ordered the shutdown of the defendants' businesses pending trial.

Credit Card Numbers Purchased

In November 1997, the three purchased access to a database of credit card information from Charter Pacific Bank of Agoura Hills, California, containing the date of sale, card number, and dollar amount of every Visa and Mastercard transaction processed through any merchant of Charter Pacific during the previous 11 months.

The FTC argued that the defendants illegally used the purchased account numbers to place charges on the accounts. The court agreed, saying, "The Court finds that the FTC has proven by a preponderance of the evidence that 90.8 percent of the total 'sales' amount the defendants caused to be deposited into their merchant accounts was unauthorized."

The defendants had access to the database of over 3.6 million card numbers through December 1998. The total amount of bogus charges was $43 million.

U.S. District Court Judge Audrey B. Collins said, "The only reasonable inference the Court can draw from the corporate defendants' access to the Charter Pacific Positive Database and the time of the defendants' fraudulent billing practices is that the defendants stole and processed Visa and MasterCard numbers from the database."

One Step Ahead of Monitoring

The defendants' questionable business practices came to the attention of Visa USA in late 1997, when they were placed on

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

MIKE HATCH, ATTORNEY GENERAL
FOR THE STATE OF MINNESOTA

Plaintiff,

vs.

US BANK NATIONAL ASSOCIATION ND f/k/a/ FIRST BANK OF SOUTH DAKOTA (NATIONAL ASSOCIATION), US BANCORP INSURANCE SERVICES, INC. and US BANCORP f/k/a FIRST BANK SYSTEMS, INC.

Defendants.

Civil Action
File Number _____

COMPLAINT

JURY TRIAL REQUESTED

PRELIMINARY STATEMENT

1. The State of Minnesota, by its Attorney General, Mike Hatch, brings this action for injunctive relief and damages based upon Defendants' violation of the Fair Credit Reporting Act, 15 U.S.C. §§ 1681 *et seq.* (FCRA) (1998). Plaintiff also seeks relief for its pendent state law claims, actual damages, punitive damages, costs, and attorney fees. Minn. Stat. §§ 325F.69; 325F.67; and 325D.44 (1998). A copy of this complaint was served upon the Office of the Comptroller of the Currency, the administrator for National Banks and the Federal Trade Commission prior to the filing of this action as required by 15 U.S.C. § 1681s (c)(2).

2. Defendants US Bank National Association ND and its parent holding company, US Bancorp, have sold their customers' private, confidential information to MemberWorks, Inc., a telemarketing company, for $4 million dollars plus commissions of 22 percent of net revenue on sales made by MemberWorks.

3. Using the personal, confidential information provided by Defendants, MemberWorks markets membership service programs to Minnesota consumers. These programs have membership fees payable monthly or annually depending on the program, ranging from approximately $50 per year to approximately $120 per year. MemberWorks refuses to provide written information about its programs until after the consumer actually enrolls in the program. Consumers generally receive a trial 30 day membership. If the membership is not canceled during the trial period, the consumer is automatically charged the annual membership fee. The fee is charged to the consumer's US Bank

10. MemberWorks Incorporated (MemberWorks), not a Defendant in this case, is a publicly traded telemarketing company based in Stamford, Connecticut. MemberWorks is not affiliated with any of the Defendants.

11. This Court has jurisdiction over this matter based upon 28 U.S.C. § 1331, in that this dispute involves predominant issues of federal law. Defendants are liable pursuant to provisions of the FCRA, 15 U.S.C. § 1681, *et seq.* Defendants are also liable pursuant to the laws of Minnesota which claims may be brought under the pendant jurisdiction of this Court.

TRIAL BY JURY

12. The State of Minnesota is entitled to and hereby requests a trial by jury. US Const. amend. 7. Fed. R. Civ. Pro. 38.

REQUEST FOR EXEMPLARY/PUNITIVE DAMAGES

13. The State of Minnesota respectfully requests that this Court instruct the jury, as the trier of facts, that in addition to actual or compensatory damages, punitive or exemplary damages may be awarded against Defendants under federal and state laws.

GENERAL FACTUAL BASIS FOR CMPLAINT

Contracts with MemberWorks

14. On or about November 1, 1996 First Bank entered into an agreement with MemberWorks, a telemarketing company based in Stamford, Connecticut, to provide MemberWorks with confidential information about the bank's consumer depositors and credit cardholders for telemarketing purposes. Appendix 1. The agreement was amended on April 12, 1999 to reflect the name change of First Bank to US Bank. Appendix 2. A second marketing agreement between US Bancorp Insurance Services, Inc., a subsidiary of US Bancorp, and Coverdell & Company, a subsidiary of MemberWorks, was made on June 30, 1998. Appendix 3.

15. These agreements permit and require Defendants to transmit confidential, personal information about their customers which the Defendants have assembled on their own and from other sources to MemberWorks. According to US Bank, this information includes but is not limited to:

a. name, address and telephone numbers of primary and secondary customers
b. checking account numbers
c. credit card numbers
d. social security numbers
e. date of birth
f. account status and frequency of use
g. gender
h. marital status
i. homeowner
j. occupation

19. The information provided by Defendants to MemberWorks includes information, such as the bankruptcy score, behavior score and various account data, including last purchase date on credit card transactions, that is at least in part based on information Defendants received from sources other than Defendants' first-hand experience with their customers. US Bank's Responses to Interrogatories and Document Requests Interrogatory No. 3, Appendix 5.

20. Since January 1, 1996 US Bancorp and its companies have provided MemberWorks with information relating to 600,000 checking account customers from Midwestern and Western states. Defendants are unable to identify how many of these 600,000 customers are from Minnesota. US Bank's Response to Interrogatory No. 7, Appendix 5.

21. Since January 1, 1996 US Bancorp and its companies have provided MemberWorks with information on approximately 330,000 of its US Bank Minnesota credit card customers. US Bank's Response to Interrogatories and Document Requests Interrogatory No. 7, Appendix 5.

22. Using the private, confidential information provided by Defendants, MemberWorks and/or its agents conduct telephone and direct mail solicitations of customers of US Bancorp and its companies. MemberWorks hires telemarketing vendors to conduct the telemarketing solicitations. These vendors, in turn, are also provided with personal, confidential information that Defendants provide to MemberWorks. Appendix 1, Attachment II, 1.a.

23. Under the terms of the contracts, Defendants review and approve the telephone solicitation scripts in advance of telemarketing solicitations. Appendix 1, Attachment II, 1.a. (2).

24. The telemarketing scripts used by MemberWorks and approved for use by Defendants direct telemarketing representatives to enroll customers in MemberWorks' programs before any literature about programs can be sent to the consumers. MemberWorks explicitly prohibits its telemarketing representatives from sending information to customers without their initial enrollment.

1. 'Send me literature'

> Mr(s)_____, I'm unable to send any information without an enrollment. That's why we've arranged to send the information out and provide you with the 30-day trial membership. If you feel the service is not for you, simply call us before the end of your 30-day trial and you won't be billed, OK!!!

See also MemberWorks Essential Scripts, Jan. 27, 1998, p.10, Appendix 11; MemberWorks CountryWide Dental scripts June 3, 1997, p. 9, Appendix 10.

25. Minnesota customers who are telemarketed by MemberWorks and its agents are unaware at the time of the solicitation that their credit card numbers and/or checking account numbers are already in the telemarketers' possession. Affidavit of Catherine

34. NACHA Rules require that debit entries to consumers' accounts must have been authorized in writing, signed or similarly authenticated by the consumers. As used by NACHA, the term "similarly authenticated" includes the use of a digital signature or other code. To meet the requirement that an authorization be in writing, an electronic authorization must be able to be displayed on a computer screen or other visual display that enables the consumers to read the communication. NACHA Rules, Article Two Subsection 2.1.2.

35. Defendants do not require MemberWorks to comply with the written authorization requirements for electronic funds transfer. In fact, Defendants have specifically contracted and/or established the practice of requiring only verbal authorization in order to approve the electronic funds transfer. This violates both federal law and NACHA Rules that protect consumers from unauthorized electronic fund transfers.

Consumer Representations

36. US Bank and US Bancorp informed consumers through advertising that the information the consumers provide Defendants will be considered confidential. Appendix 12.

37. Defendants have informed customers that they will only disclose information in certain circumstances:

Disclosure of Account Information
Information concerning your account and your account transactions, including electronic banking transactions, may be released to third parties only under the following circumstances:

- in connection with an examination by government regulators or external auditors;
- to comply with a request for information from a party to whom you have given our name as a reference or a party to whom you have written a check or otherwise agreed to make payment from your account;
- to report to (a) a credit bureau about the existence or condition of your account or (b) an information clearinghouse if we close your account due to excessive overdrafts or other irregular activity by you;
- to any person to whom you have given information about your account (such as your account number and personal identification number) that is enough to permit them to pose as you;
- to comply with a subpoena or any other legitimate request under state or federal law;

- when we need to in order to complete transactions, including electronic banking transactions;
- when we conclude that disclosure is necessary to protect you, your account or our interests; or
- if you give your written permission.

38. US Bank and US Bancorp do not disclose to their customers that they routinely

and telemarketing solicitations to Minnesota customers.

45. MemberWorks sells the membership program Countrywide Dental and Health service for an introductory price of $89.95 per year and an annual renewal price of $99.95 per year, payable in monthly renewals of $8.95. The program promises free or nominal charge for X-ray and oral exams, discount pricing for dental work and access to a network of participating dentists along other benefits. This program was marketed to US Bank customers.

46. MemberWorks sells its membership programs for various prices which are set forth in the Membership Program. Appendix 9.

47. MemberWorks' programs are set up to offer either periodic monthly payment of fees or annual payment of fees. Appendix 9.

48. MemberWorks markets its program offering the customer a 30-day trial period. In its initial contact with Defendants' customers, MemberWorks asserts that it obtains verbal authorization to make a monthly deduction from the customer's checking account or a billing to the customer's US Bancorp credit card. Appendix 10, page 5.

49. Notice that MemberWorks will begin automatically deducting fees from the customer's checking account or billing the credit card is sent to Minnesota customers on a postcard. A copy of this postcard is attached as Appendix 8.

50. Neither MemberWorks nor Defendants obtain written authorization for electronic deductions from consumers' checking accounts.

51. Defendants' contracts with MemberWorks require Defendants to refer all consumer complaints to MemberWorks.

COUNT I

VIOLATION OF FAIR CREDIT REPORTING ACT

52. Plaintiff incorporates and realleges paragraphs 1-50.

53. By assembling and transmitting consumer reports (15 U.S.C. § 1681a(d)(1)) that is at least in part obtained from other sources, Defendants are a "credit reporting agency" as that term is defined by the FCRA. 15 U.S.C. § 1681a(f).

54. In the course of its actions, Defendants have willfully and/or negligently violated the provisions of the FCRA in the following respects:

a. By willfully and/or negligently failing to provide consumer reports for a permissible purpose as required by § 1681b of the FCRA.
b. By willfully and/or negligently failing to maintain reasonable procedures to ensure proper disclosure of information to third parties as required by §1681e.
c. By willfully and/or negligently failing to maintain reasonable procedures to ensure compliance with consumer disclosure obligation as required by § 1681g.

confidential information in a paragraph titled "Affiliate Sharing" (i.e. other legal entities that are part of Defendants' corporate family). By titling the paragraph "Affiliate Sharing," consumers are deceived and/or misled regarding the sale of information to unrelated, non-affiliated entities. Appendix 15.

66. Defendants' failure to require or obtain written authorization prior to electronic transfer of funds violates both the Electronic Funds Transfer Act, Reg. E and NACHA Operating Rules and is thus a violation of Minnesota's Prevention of Consumer Fraud Act.

67. Defendants approved the use of deceptive and misleading telemarketing practices, including the refusal to provide literature to consumers without a prior sale and misrepresentations about the transfer of account numbers of bank customers to MemberWorks by Defendants.

68. Defendants' sale of personal, confidential information obtained from consumers in the course of a banking relationship violates Minnesota consumers' common law right to privacy and is a deceptive and misleading act. *Lake v Wal-Mart Stores, Inc.*, 582 N.W.2d 231 (Minn. 1998).

69. The Defendants' intentional intrusion upon the private affairs or concerns through the sale of confidential information is highly offensive to a reasonable person.

70. Defendants' appropriation of its customers' personal and confidential information for its own use or benefit violates the common law right to privacy.

71. Defendants' publication of Minnesota consumers' private facts to third parties is highly offensive to a reasonable person. The publication of these private facts concerns matters which are not of legitimate concern to the public.

72. The privacy interests of Minnesota consumers in the confidentiality of their personal financial information affects the economic health and well-being of Minnesota residents.

73. Defendants' conduct has adversely affected hundreds of thousands of Minnesota citizens living in every county in the State of Minnesota.

74. The systematic violation of Minnesota consumers' common law right of privacy is a violation of Minnesota's Prevention of Consumer Fraud Act and Deceptive Trade Practices Act.

75. Defendants' conduct described in the above paragraphs 1-74 constitutes multiple, separate violations of Minn. Stat. § 325F.69, subd. 1 (1998).

COUNT III

VIOLATIONS OF MINN. STAT. § 325F.67 (1998)

FALSE ADVERTISING

82. Defendants' approval of telemarketing scripts that fail to accurately convey the data Defendants have sold to MemberWorks deceives Minnesota consumers and creates significant confusion and misunderstanding.

83. Defendants' failure to require or obtain written authorization prior to electronic transfer of funds violates both the Electronic Funds Transfer Act, Reg. E and NACHA Operating Rules, and is thus a violation of Minnesota's Deceptive Trade Practice Act.

84. Defendants' sale of personal, confidential information obtained from consumers in the course of a banking relationship violates Minnesota consumers' common law right to privacy, and it is a deceptive trade practice. *Lake v Wal-Mart Stores, Inc.*, 582 N.W.2d 231 (Minn. 1998).

85. Defendants' conduct as described in the above paragraphs 1-84 constitutes multiple, separate violations of Minn. Stat. § 325D.44, subd. 1 (5) and (13) (1998).

RELIEF

WHEREFORE, Plaintiff, the State of Minnesota, by its Attorney General, Mike Hatch, respectfully asks the Court to award judgment against Defendants:

1. Declaring that Defendants' acts and practices described in this complaint constitute multiple, separate violations of the Fair Credit Reporting Act. 15 U.S.C. § 1681 et seq.
2. Declare that Defendants' acts and practices described in this complaint constitute multiple, separate violations of Minnesota's Prevention of Consumer Fraud Act. Minn. Stat. § 325F.69.
3. Declare that Defendants' acts and practices described in this complaint constitute multiple, separate violations of Minnesota's False Advertising Act. Minn. Stat. § 325F.67.
4. Declare that Defendants' acts and practices described in this complaint constitute multiple, separate violations of Minnesota's Deceptive Trade Practices Act. Minn. Stat. § 325D.44.
5. Enjoining, via the entry of a preliminary and permanent injunction, Defendants from engaging in the practices alleged in this Complaint and violating the above statutes. 15 U.S.C. § 1681s.
6. Awarding damages on behalf of the residents of the State of Minnesota as the result of willful and negligent violations of the FCRA §§ 1681n and 1681o.
7. Requiring Defendants make restitution in an amount to be determined by the Court and awarding judgment against Defendants for such amount.
8. Ordering Defendants to take such remedial measures as the Court deems appropriate.
9. Awarding judgment against Defendants and civil penalties pursuant to Minn. Stat. § 8.31, subd. 3 (1998).
10. Awarding Plaintiff its costs, including costs of investigation and reasonable attorney fees, as authorized by Minn. Stat. § 8.31, subd 3a (1998) and the FCRA.
11. Granting such further legal or equitable relief as the Court deems appropriate and just.

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

MIKE HATCH, ATTORNEY GENERAL
FOR THE STATE OF MINNESOTA

Plaintiff,

vs.

US BANK NATIONAL ASSOCIATION ND f/k/a/ FIRST BANK OF SOUTH DAKOTA (NATIONAL ASSOCIATION), US BANCORP INSURANCE SERVICES, INC. and US BANCORP f/k/a FIRST BANK SYSTEMS, INC.

Defendants.

Civil Action
Court File No. 99-872 adm/ajb

FINAL JUDGMENT AND ORDER FOR INJUNCTIVE AND CONSUMER RELIEF

The above-entitled matter came before the undersigned Judge of District Court on _____, 1999 upon the parties' joint application, based on a Stipulation of Settlement between the parties. Plaintiff State of Minnesota appeared by Deputy Attorney General Lori R. Swanson. Defendants appeared by Richard B. Solum, Esq.

Based upon the Stipulation of the parties, and upon all the files, records and proceedings herein,

IT IS HEREBY ORDERED AND DECREED:

PRELIMINARY MATTERS

1. The above-named Court has jurisdiction over the subject matter of this case, having federal question jurisdiction over the claims asserted under 15 U.S.C. section 1681 and having supplemental jurisdiction over the remaining state law claims.

2. The parties consent and agree to the Court's entry of this Order.

3. This Order is in the public interest.

DEFINITIONS

r. account customer's behavior score

s. account customer's bankruptcy score

t. account customer's date of last payment

u. account customer's amount of last payment

v. account customer's date of last statement

w. account customer's statement balance

"Customer Data" shall not include such information (1) to the extent contained in reports provided to employers of cardholders who are issued credit cards by Defendants or their Affiliates as part of a program for business, travel, purchasing, corporate or other similar cards instituted between Defendants or their Affiliates and such employers; or (2) with respect to employees of Defendants or their Affiliates, in connection with discounts or special buying programs for non-Financial Products or Services negotiated by and offered to employees of Defendants or their Affiliates.

7. "Minnesota Customer" means any natural person who, since June 1, 1997, had a credit card or depository agreement with U.S. Bancorp or its Affiliates and either had a Minnesota address or was a Minnesota resident at the time such agreement was in effect.

8. "Defendants" means U.S. Bancorp and its Affiliates.

9. "Direct Marketing" means telemarketing and targeted direct mail solicitations (and does not include solicitations accompanying statements or other account servicing communications.)

10. "Financial Products or Services" means securities or insurance products or services which are subject to regulation under federal or state securities or insurance laws; the making of loans or extensions of credit of all types and related services which are reasonably necessary to carry out the making of the loan or extension of credit (e.g. closings, filings, appraisals, title examinations); leasing (provided that the disclosure of Customer Data pursuant to an agreement with an Unaffiliated Third Party shall not be termed a "lease" of such data); and trust and asset management services.

ORDER

11. Defendants and their Affiliates shall not share Customer Data with Unaffiliated Third

to notify at least 90 percent of such customers, their notification efforts shall be presumed to be not reasonable, in which case the Court or special master may order further efforts at notification. The notice to customers shall apprise them of a dedicated toll-free customer service number and their right to obtain further information from the Minnesota Attorney General's Office at (651) 296-3353 or (800) 657-3787. All costs associated with the notice, refund and fees of the retired judge shall be paid by Defendants.

19. In addition to the disclosure required in paragraph 14, Defendants shall conspicuously and clearly, in written communications, disclose their privacy policy to their individual (natural person) customers:

a. Defendants shall make all reasonable efforts to provide a written disclosure to each such customer when the customer initially purchases any product provided by Defendants (or promptly thereafter if the purchase is not made in person.)

b. The disclosure shall thereafter be given at least annually.

c. The above disclosures shall clearly list each category of information the Defendants propose to share with any Affiliate for Direct Marketing Purposes, or Unaffiliated Third Party for purposes of marketing Financial Products or Services of the Unaffiliated Third Party, and the specific purpose for the sharing of information, disclosed in separate paragraphs as it relates to Affiliates and Unaffiliated Third Parties.

d. Each privacy disclosure shall provide such customers with an easily available method to "opt-out" of the sharing of Customer Data with Affiliates for Direct Marketing purposes and with Unaffiliated Third Parties for purposes of marketing Financial Products or Services of the Unaffiliated Third Party. The "opt-out" system shall include both toll-free telephone numbers and addresses where customers may notify the Defendants of their desire to "opt-out" of such sharing of Customer Data. Defendants shall also accept "opt-out" notices submitted to tellers or other consumer representatives. Simple "opt-out" forms shall be made available in conspicuous public locations in each branch office of U.S. Bank. The form of such disclosure documents shall be filed with and approved by the OCC.

on such successor corporation's affiliates, provided that the transaction value at the time of the announcement of such merger is an amount equal to 25 percent of the pre-announcement market capitalization of U.S. Bancorp; in such event, however, the successor corporation and its affiliates shall comply with any then-existing applicable laws.

(D) In the event new federal legislation or regulation applicable to national banks and respecting the specific subject matter of any paragraph herein is passed or adopted, Defendants may provide written notice to the Minnesota Attorney General's Office that they believe that such new federal legislation or regulation should result in a modification of this Order. If the Attorney General's Office fails within 30 days to notify Defendants in writing that it disagrees with Defendants' notice, then such modification as specified in Defendants' notice shall be deemed effective with no further judicial action. However, in the event the Attorney General's Office notifies Defendants in writing within the 30 day period that it disagrees with Defendants' notice, then Defendants may petition on 30 days notice to the Minnesota Attorney General's Office the Court for a modification such that this Order is no more restrictive than the minimum requirements of such new laws or regulations.

(E) Defendants may petition the Court for a modification of this Order in the event that the OCC should impose upon these Defendants specifically any obligation which renders Defendants reasonably unable to comply with any provision of this Order.

LET JUDGMENT BE ENTERED ACCORDINGLY.

BY THE COURT:

Dated: _____ UNITED STATES DISTRICT COURT

_____

The Honorable James M. Rosenbaum

Judge of District Court

THE ATTORNEY GENERAL OF THE STATE OF NEW YORK
BUREAU OF CONSUMER FRAUDS AND PROTECTION

IN THE MATTER OF

CHASE MANHATTAN BANK USA, N.A.

ASSURANCE OF DISCONTINUANCE PURSUANT TO EXECUTIVE LAW §63(15)

Pursuant to the provisions of Article 22-A of the General Business Law ("GBL") and Section 63(12) of the Executive Law, Eliot Spitzer, Attorney General of the State of New York State, caused an inquiry to be made into certain marketing practices of Chase Manhattan Bank USA, N.A. Based upon this inquiry, the Attorney General makes the following findings:

FINDINGS OF FACTS

1. Chase Manhattan Bank USA, N.A. is a subsidiary of The Chase Manhattan Corporation. Its principal place of business is located at 802 Delaware Avenue, Wilmington, Delaware 19801. Chase Manhattan Bank USA, N.A. and The Chase Manhattan Corporation are herein referred to as "Chase".

2. Chase is a credit card issuer and has approximately 20 million accounts nationwide. Chase also holds a substantial number of residential mortgages.

3. Chase has engaged in marketing programs with major nonaffiliated telemarketing and direct mail entities for the purpose of offering consumer products and services to its

particular product or service to be offered, the nonaffiliated third party vendor arranged for telemarketing or direct mail representatives to have access to the list of cardholder names, addresses and telephone numbers of those specific Chase customers in order to conduct telephone and/or direct mail solicitations.

7. Chase customers who were contacted by nonaffiliated third party vendors and/or their agents had not been advised of the specific types of information that had been in the possession of the nonaffiliated third party vendor.

8. On or about July 1, 1999, Chase voluntarily imposed a moratorium on such marketing efforts.

9. At the time of the opening of a credit card account and periodically thereafter, Chase provided its cardholders with a copy of its "Customer Information Principles" which set forth its policies for protecting the privacy and confidentiality of customer information. Chase informed customers, inter alia, that it does not share information about its customers with unrelated companies except in certain limited circumstances, including making available special offers of products and services that it felt may be of interest to Chase customers. Chase provided a similar statement of its "Customer Information Principles" in its initial welcome kit for Chase customers who had obtained mortgages from Chase.

10. Chase did not include information on how to opt-out in its initial notice to mortgagors and did not include information on opting-out on its website or identify in its opt-out notice to credit card holders an 800 number by which consumers can opt-out.

11. The Attorney General believes that Chase has not fully and adequately disclosed to Chase customers that specific types of information on the computer tapes were provided to

and in subsequent disclosures to Chase customers and was consistent with its stated intention to make available products and services that Chase believed would be of interest to Chase customers and that information about Chase customers was appropriately protected by the terms of its confidentiality agreements with the nonaffiliated third party vendors. Chase provided additional information regarding information sharing when it notified customers with Chase credit card accounts that the customers could inform Chase that they did not want to receive telemarketing calls or direct mail solicitations. A welcome kit informed Chase credit card customers that they could opt-out at any time by contacting Chase at a specified 800 number. Chase also published its customer information principles online at its website at www.chase.com. Chase has further stated that information about Chase customers was not provided to nonaffiliated third party vendors if the Chase customers had exercised their opportunity to opt-out and that the opportunity to opt-out was clear, the means to do so was easily accessible to customers and the opt-out was, in fact, exercised by Chase customers. Chase further states that the identity of the stores or other providers at which cards were used and the specific purchases made were not disclosed to the nonaffiliated third party vendor and that the individuals making telemarketing calls to Chase customers did not have access to information regarding the credit balance or credit line, or regarding the extent or timing of the Chase customers' use of their credit cards or the identity of the stores or other providers at which cards were used or the specific purchases made.

IT NOW APPEARS that Chase is willing to enter into this Assurance without admitting that it has violated any law, or that it otherwise committed any wrongful or improper act and further without admitting that the alleged practices violate New York state consumer

information principles, including a description of the types of entities to which the Chase customer's name, address and telephone number is provided and a notice that such information may be shared for the purpose of telemarketing and/or direct mail solicitations unless the customer directs that such information not be disclosed to such nonaffiliated third party vendors, and (ii) gives the customer notice that the customer may direct Chase not to disclose his/her name, address and phone number to nonaffiliated third party vendors by writing to Chase at a designated address or by calling Chase at a specified toll-free number ("Opt-Out Notice"). The Opt-Out Notice shall be set apart from the text of the customer information principles, shall be headed Opt-Out Notice, or words of similar import and meaning, such heading to be in at least 12 point bold type and the body of the Notice shall be in at least 9.5 point type. Chase shall further publish its customer information principles and method for opting-out on its website.

3. This Assurance shall not apply, either before or after the effective date of the Gramm-Leach-Bliley Act signed into law by the President on November 12, 1999, to the disclosure of customer information in accordance with the provisions of Sections 502(b)(2), 502(e) or 504(b) of the Gramm-Leach-Billey Act, as originally enacted or as it may later be amended, or in accordance with any regulations which may from time to time be promulgated thereunder; except that, nothwithstanding the foregoing, this Assurance shall apply (i) to any marketing program that was in existence on June 15, 1999 and was on the list of programs supplied to the New York Attorney General's office by Chase, or (ii) to any similar program involving the sharing of customer information with a nonaffiliated third party vendor that is not a financial institution (as that term is defined in the Gramm-Leach-Bliley Act) for the purpose of marketing such vendor's products. However, Chase may continue to provide customer information to those

which Chase must comply with regulations adopted pursuant to the Gramm-Leach-Bliley Act indicating the manner and extent of its compliance with this Assurance of Discontinuance and shall annex thereto copies of its revised customer information principles and Opt-Out Notices to customers.

9. Nothing contained herein shall be construed as to deprive any individual of any private right of action under the law. This Assurance shall not confer on any person any rights as a third party beneficiary or otherwise against Chase.

10. Chase shall pay to the Attorney General within 10 days of the execution of this Assurance the sum of $101,500 as costs of this investigation pursuant to Executive Law §63(15).

11. Pursuant to Executive Law § 63(15), evidence of a violation of this Assurance shall constitute prima facie proof of a violation of the applicable statutes in any

CORPORATE ACKNOWLEDGMENT

STATE OF DELAWARE)
: ss
COUNTY OF)

, being duly sworn, deposes and says:

I am a corporate officer of Chase Manhattan Bank USA, N.A., the entity described in and which executed the foregoing Assurance of Discontinuance. I have executed the aforesaid instrument with the consent and authority of Chase Manhattan Bank USA, N.A. and those responsible for the acts of said entity and duly acknowledge same.

Sworn to before me this
day of January, 2000

Notary Public

Settlement with Discount Buying Club Highlights Privacy Concerns

Olympia - Aug. 4, 2000 - A settlement reached today with a Connecticut-based merchandiser of discount buying clubs is a victory for consumers, and highlights the need for strong legislative action to protect consumers' private financial information, Attorney General Christine Gregoire said.

The settlement with BrandDirect will require the company to pay $1.9 million in penalties, fees, and consumer education funds, and about $11 million in restitution to settle a lawsuit accusing the company of charging consumers for buying-club memberships without permission and engaging in other deceptive and unfair practices.

The Washington and Connecticut Attorneys General filed the lawsuit today in Federal District Court in Connecticut. It alleged that the company, which is partly owned by Reader's Digest and Federated Department Stores, violated federal telemarketing law and the two states' consumer protection laws.

BrandDirect uses information provided by some of the nation's largest financial institutions, including First USA Bank, CitiBank, Chase Manhattan Bank and others, to develop lists of consumers who are then called by telemarketers. Consumers are offered an opportunity to join discount-buying clubs that cater to consumers' particular interests.

For example, the Simplicity Sewing and Crafts Club is a discount buying club that caters to people who like to sew, and the Best Friends Pet Club caters to pet owners.

BrandDirect obtains consumers' charge card information from the banks, allowing BrandDirect to conveniently bill consumers who agree to join. In some instances, however, the information is used to make unauthorized charges against consumers' accounts, Gregoire said.

"In this case, banks, without the consent of their customers, shared credit card information with an over-zealous marketing firm, which misled, overcharged and underdelivered to Washington consumers," Gregoire said.

"This is a classic case illustrating why consumers have a right to worry about what is happening to their private information. Without their consent, personal information for more than 60,000 Washington consumers was sold to a firm which we contend regularly violated federal and state consumer protection

Agreement with Citibank Will Safeguard Consumer Financial Information

OLYMPIA- 2/27/02 - An agreement between Citibank and several states, including Washington, will result in new restrictions on the use of personal financial information that the bank shares with direct marketers, Attorney General Christine Gregoire announced today.

The agreement-signed by representatives of Citibank, Washington, 26 other states and Puerto Rico -is the latest in a series of efforts by state attorneys general to control how telemarketing and other direct sales firms use credit-card numbers and other personal information obtained from financial institutions, Gregoire said.

"Consumers should be able to trust that their personal financial information will be handled as carefully as their savings deposits," Gregoire said. "Citibank has accepted responsibility for the marketing practices of the businesses it shares information with. Hopefully, other financial institutions will follow Citibank's lead."

Information sharing by banks has led to consumer complaints about the appearance of unauthorized charges on their credit cards. In those cases, consumers complained they were unaware telemarketers had their financial information.

The agreement with Citibank spells out conditions it will impose on businesses with whom it shares customer information. The conditions require:

- Bank review and approval of all marketing materials;
- Compliance with all consumer protection laws by telemarketers;
- Clear approval by cardholders prior to any charges.

The agreement also bans deceptive marketing and, if telemarketers mention the bank during a sales call, they must clearly state they are not affiliated with the bank.

The Citibank agreement follows similar agreements with two other firms. Those agreements also were intended to curb the improper use of personal financial information shared by financial institutions.

In August 2000, the state settled a case with the Connecticut-based telemarketing firm BrandDirect, which had obtained consumer information from several major financial institutions, including Citibank. Consumers

Press Releases
Office of New York State Attorney General Eliot Spitzer

Department of Law
120 Broadway
New York, NY 10271

For More Information:
(518) 473-5525

Department of Law
The State Capitol
Albany, NY 12224

For Immediate Release
September 18, 2000

NATIONAL TELEMARKETING FIRM TO REFORM PRACTICES

Bank Privacy Investigations Result in Settlement On Unauthorized Credit Card Charges

Attorney General Eliot Spitzer today announced a settlement with a national telemarketing company that will protect consumers from unauthorized credit card charges and require full and clear up-front disclosures in sales representations.

MemberWorks, Inc., a Stamford, Connecticut-based company, settled allegations of telemarketing abuses in connection with its sales of lifestyle club memberships which offer consumers alleged savings on a variety of products and services involving entertainment, shopping, home improvement, and health care. It is estimated that the company has more than 600,000 customers in New York State.

This settlement arose from the Attorney General's continuing investigation of banks and credit card issuers that violated their cardholders' privacy rights by selling their personal account information to telemarketers in return for a substantial commission.

"This agreement reaffirms the need for aggressive oversight of privacy-related issues and the need for tight control over access to financial information such as credit card numbers," Spitzer said. "The reforms provided in this settlement will ensure more complete and accurate disclosures in telemarketing campaigns so that consumers can make informed decisions."

Attorney General Spitzer said that MemberWorks entered into agreements with Citibank, its largest client, and other major financial institutions that provided customer names and account information. This information was used in telemarketing campaigns to lure consumers with a "free 30-day trial membership" in one of its many membership clubs. At the end of the trial period, MemberWorks charged many of its customers' credit card accounts an annual fee of between $60 and $144, without their knowledge or authorization, for the membership using credit card numbers provided by the consumer's financial institution.

MemberWorks made wide use of negative option plans with its "risk free" 30-day free trial membership offer. Although these plans offer

THE CHAIRMAN

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

April 24, 2002

The Honorable John McCain
Committee on Commerce, Science, and Transportation
United States Senate
Washington, D.C. 20510-6125

Dear Senator McCain:

Thank you for your letter of April 19, 2002, requesting my views on S.2201, the Online Personal Privacy Act.

Personal privacy issues are a key priority at the Commission. Because a variety of practices can have negative consequences, consumer concerns about privacy are strong and justified. Avoiding these consequences requires a strong law enforcement presence, and we have increased by 50 percent FTC resources targeted to addressing privacy problems. Our agenda includes:

- A proposed rulemaking to establish a national, do not call registry;
- Greater efforts to enforce both online and offline privacy promises;
- Beefed up enforcement against deceptive spam;
- A new emphasis on assuring information security;
- Putting a stop to pretexting;
- Increased enforcement of the Children's Online Privacy Protection Act; and
- New initiatives to both help victims of I.D. theft and assist criminal prosecution of this crime.

The concerns about privacy that motivate our enforcement agenda have led others, including many members of Congress, to propose new laws, such as S.2201, the Online Personal Privacy Act. There are potential benefits from general privacy legislation. If such legislation could establish a clear set of workable rules about how personal information is used, then it might increase consumer confidence in the Internet. Moreover, federal legislation could help ensure consistent regulation of privacy practices across the 50 states. Although we should consider carefully alternative methods to protect consumer privacy and to reduce the potential for misuse of consumers' information, enactment of this type of general legislation is currently unwarranted.[1]

Five points underscore my concern about general, online privacy legislation:

1. Drafting workable legislative and regulatory standards is extraordinarily difficult.

The recently-enacted Gramm-Leach-Bliley Act ("GLB"), which applies only to financial institutions, required the multiple mailings of over a billion privacy notices to consumers with little current evidence of benefit.[2] Our experience with GLB privacy notices should give one great pause about whether we know enough to implement effectively broad-based legislation, even if it was limited to notices.

Unlike GLB, the proposed legislation deals with a wide variety of very different businesses, ranging from the websites of local retailers whose sales cross state lines to the largest Internet service providers in the world. Thus, implementation of its notice requirement will likely be even more

complicated.

Moreover, the legislation adds requirements for access not found in GLB. The recommendations of the FTC's Advisory Committee on Online Access and Security make clear that no consensus exists about how to implement this principle on a broad scale.[3] Perhaps reflecting these same concerns, S.2201 grants the FTC broad rulemaking authority. The only legislative guidance is the requirement that the procedures be reasonable. The statute is silent, for example, on how to balance the benefits of convenient customer access to their information with the inherent risks to security that greater access would create. The FTC has no answer to this conundrum. We do not know how to draft a workable rule to assure that consumers' privacy is not put at risk through unauthorized access.

The inherent complexity of general privacy legislation raises many difficulties even with provisions that are conceptually attractive in the abstract. For example, the proposed legislation imposes different requirements on businesses based on whether they collect "sensitive" or "nonsensitive" personal information. Although this may be a conceptually sound approach, we have no practical experience in implementing it, and attempting to draw such distinctions appears fraught with difficulty, both in drafting regulations and assuring business compliance. Under the statute, for example, the fact that I am a Republican is considered sensitive, but a list of books I buy and websites I visit are not.

Similarly, the broad state preemption provision would provide highly desirable national uniformity. Questions about the scope of preemption would inevitably arise, however. How would the preemption provision affect, for example, state laws on the confidentiality of attorney/client communications for attorneys using websites to increase their efficiency in dealing with their clients? Moreover, what are the implications for state common law invasion of privacy torts when the invasion of privacy occurs online?

Another problem is that, except for provisions reconciling the provisions of this bill with the provisions of the Children's Online Privacy Protection Act and certain provisions of the Federal Communications Act, there are no provisions reconciling the proposed legislation with other important Federal privacy legislation. For example, it is unclear how S.2201's requirement of notice and "opt-in" choice for disclosure of financial information collected online would be reconciled with GLB's notice and "opt-out" requirements for the same information. Nor is it clear whether a credit reporting agency's use of a website to facilitate communications with its customers would subject it to a separate set of notice, access, and security requirements, beyond those already in the Fair Credit Reporting Act.

I want to emphasize that I note these examples, not to criticize the drafting of the proposed legislation, but to illustrate the inherent complexity of what it is trying to accomplish.

2. The legislation would have a disparate impact on the online industry.

Second, I am concerned about limiting general privacy legislation to online practices. Whatever the *potential* of the Internet, most observers recognize that information collection today is also widespread offline. Legislation subjecting one set of competitors to different rules, simply based on the medium used to collect the information, appears discriminatory. Indeed the sources of information that lead to our number one privacy complaint - ID Theft - are frequently offline. Of course, applying the legislation offline would increase the complexity of implementation, again underscoring the difficulties inherent in general privacy legislation.

3. We have insufficient information about costs and benefits.

Third, although we know consumers value their privacy, we know little about the cost of online

privacy legislation to consumers or the online industry. Again, the experience under GLB indicates that the costs of notice alone can be substantial. Under S.2201, these costs may be increased by the greater number of businesses that must comply, by uncertainty over which set of consent procedures apply, and by the difficulty of implementing access and security provisions.

4. Rapid evolution of online industry and privacy programs is continuing.

Fourth, the online industry is continuing to evolve rapidly. Recent surveys show continued progress in providing privacy protection to consumers.[4] Almost all (93 percent) of the most popular websites provide consumers with notice and choice regarding sharing of information with third parties. Some of the practices of most concern to consumers, such as the use of third party cookies, have declined sharply. Moreover fewer businesses are collecting information beyond email addresses. These changes demonstrate and reflect the more important form of choice: the decision consumers make in the marketplace regarding which businesses they will patronize. Those choices will drive businesses to adopt the privacy practices that consumers desire.

Perhaps most important for the future of online privacy protection, 23 percent of the most popular sites have already implemented the Platform for Privacy Preferences (P3P). This technology promises to alter the landscape for privacy disclosures substantially. Microsoft has incorporated one implementation of P3P in its web browser; AT&T is testing another, broader implementation of this technology. By the time the Act's disclosure regulations might reasonably take effect,[5] the technological possibilities for widespread disclosure may differ substantially. Although S.2201 anticipates this development by requiring the National Institute of Standards to promote the development of P3P technology, legislation enacted now cannot take advantage of such nascent technology. Moreover, it may inadvertently reduce the incentives for businesses and consumers to adopt this technology if disclosures are required using other approaches.

5. Diversion of resources from ongoing law enforcement and compliance activities.

Finally, there is a great deal the FTC and others can do under existing laws to protect consumer privacy. Indeed, since 1996, five new laws have had a substantial impact on privacy-related issues.[6] We should gain experience in implementing and enforcing these new laws before passing general legislation. Implementation of yet another new law will require both industry and government to focus their efforts on a myriad of new implementation and compliance issues, thus displacing resources that might otherwise improve existing privacy protection programs and enforce existing laws. Simply shifting more resources to privacy related matters will not, at least in the short term, correct this problem. The newly-assigned staff would need to develop the background necessary to deal with these often complex issues. The same is likely true for business compliance with a new law. Without more experience, we should opt for the certain benefits of implementing our aggressive agenda to protect consumer privacy, rather than the very significant effort of implementing new general legislation.

Conclusion

We share the desire to provide American consumers better privacy protection and to ensure that American businesses face consistent state and Federal standards when handling consumer information. Nonetheless, we believe that enactment of this general online privacy legislation is premature at this time. We can better protect privacy by continuing aggressive enforcement of our current laws.

Sincerely,

Timothy J. Muris
Chairman

cc:
The Honorable Ernest Hollings
Chairman, Committee on Commerce, Science and Transportation
United States Senate

1. There may be areas in which new legislation is appropriate to address a specific privacy issue. This letter addresses my concerns about broad, general legislation governing online privacy issues.

2. I am unaware of any evidence that the passage of GLB increased consumer confidence in the privacy of their financial information. In contrast to GLB's notice requirements, certain GLB provisions targeting specific practices have directly aided consumer privacy. For example, the law prohibits financial institutions from selling lists of account numbers for marketing purposes, and makes it illegal for third parties to use false statements ("pretexting") to obtain customer information from financial institutions in most instances.

3. The Committee's Final Report is available at www.ftc.gov/acoas/papers/finalreport.htm.

4. The Progress and Freedom Foundation recently released the results of its 2001 Privacy Survey, available at www.pff.org/pr/pr032702privacyonline.htm.

5. Again, GLB is instructive. It was almost two years between the enactment of the statute and the effective date of the privacy rules promulgated thereunder.

6. Fair Credit Reporting Act, 15 U.S.C. § 1681 (amended 9/30/96); Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320 (enacted 8/21/98); Children's Online Privacy Protection Act, 15 U.S.C. § 6501 (enacted 10/21/98); ID Theft Assumption & Deterrence Act, 18 U.S.C. § 1028 (enacted 10/30/98); GLB, 15 U.S.C. § 6801 (enacted 11/12/99). Moreover, since 1996, the FTC has been applying its own statute to protect privacy.

www.nytimes.com
The New York Times ON THE WEB

April 11, 2002

Seeking Profits, Internet Companies Alter Privacy Policy

By SAUL HANSELL

Pressed for profits, Internet companies are increasingly selling access to their users' postal mail addresses and telephone numbers, in addition to flooding their e-mail boxes with junk mail.

Yahoo (news/quote), the vast Internet portal, just changed its privacy policy to make it clear that it has the right to send mail and make sales calls to tens of millions of its registered users. And it has given itself permission to send users e-mail marketing messages on behalf of its own growing family of services, even if those users had previously asked not to receive any marketing from Yahoo. Users have 60 days to go to a page on Yahoo's Web site where they can record a choice not to receive telephone, postal or e-mail messages in various categories.

Similarly, when Excite, another big Internet portal, was sold in bankruptcy court late last year, the new owner asked Excite users to accept a privacy policy that explicitly allows it to rent their names and phone numbers to marketing companies. (Those users, too, could check a box on the site to opt out of such programs, if they had not already done so on the old Excite.)

The sites say that direct marketing to their users, both by e-mail and by older means, is an important source of revenue that can help make up for the rapid decline in sales of online advertising.

"It has been our orientation from the beginning to be straightforward with the user," said Bill Daugherty, the co-chief executive of the Excite Network. "They are getting free content and utility that is unparalleled, and in return we will be marketing products to them."

But even many marketing experts say that the risk to the reputations of these companies may outweigh any revenue they may receive.

"What Yahoo has done is unconscionable," said Seth Godin, Yahoo's former vice president for direct marketing. "It's a bad thing, and it's bad for business. They would be better off sending offers to a million people who said they want to receive a coupon each day than to send them to 10 million people and worry about whether you have offended them by finally going too far." While at Yahoo, Mr. Godin published "Permission Marketing" (Simon & Schuster, 1999), which argued that marketing messages should be sent only to people who ask to see them.

Both Yahoo and Excite say they are not loosening their privacy policies, just making them more explicit. In the past, both companies simply asked users to check a box authorizing the Web sites to "contact" them with marketing messages. The sites assert that such wording did not rule out mail and telephone contacts in addition to e-mail messages.

Privacy experts say such a legalistic interpretation of the privacy policy is at best misleading because, in practice, almost all contact from the sites has been by e-mail. "It's unfair," said Mark Rotenberg, executive director of the Electronic Privacy Information Center. "People thought they were going to get e-mail solicitations. They didn't expect that their dealings with Yahoo would cause them to receive phone calls."

Both Yahoo and Excite say they have not actually used users' phone numbers for any marketing programs so far and have made relatively few mailings to members.

Other sites have been much more liberal in renting customer names. America Online, the biggest Internet service, has long rented customer addresses, and it also calls users to promote its services and those of its business partners. Lycos, the big Internet portal, and CNET's ZDNet, a technology site, also rent users' names through mailing-list brokers.

For example, Direct Media, a mailing list broker in Greenwich, Conn., offers access to 2.9 million Lycos users at a cost of $125 per thousand names for a single mailing. (An extra $15 per thousand lets marketers select users showing an interest in a topic like cats or gambling.) Advertisers typically pay for the right to send a single mailing or make a single phone call to a name on a list they rent; they do not own the information outright.

Stephen J. Killeen, the United States president of Terra Lycos (news/quote), the parent of the Lycos portal, said mailing list rentals were a small but growing part of its marketing revenue. It does not yet rent phone numbers, a service that has a smaller market. "We look at ourselves as a way to match the right consumer with the right product, whatever the medium," Mr. Killeen said. "A lot of advertisers are looking at the Internet as part of integrated marketing campaigns."

The privacy policy of Microsoft (news/quote)'s MSN portal lets it send mail and make phone calls to customers on behalf of advertisers, but it has yet to do so. Microsoft lets users specify whether they do not want marketing via e-mail, postal mail or phone.

"We value our customers' privacy," said Brian Gluth, a senior product manager at MSN, "and we have never changed a customer's preference of opt-in or opt-out, like some of our competitors have done."

In many ways the Internet is simply joining the mainstream of American business, where the names of people who subscribe to magazines and who buy from catalogs are freely traded.

Steven Sheck, the president of Infinite Media, a mailing list broker in White Plains, said he was seeing an increase in the number of Web sites renting access to users' names.

"Given the state of the economy," he said, "Internet companies are looking at their customer lists as an asset with which they can generate revenue."

Yahoo says its move to send mail and make calls to users on behalf of advertisers is far more limited than simply renting its customer file to companies with no relationship to Yahoo. It compares itself with American Express (news/quote), which has long sent offers to cardholders for its own services, like insurance, and for those of other companies, like airlines and department stores.

"To the extent we have been successful," said Lisa Nash, Yahoo's director of consumer and direct marketing, "it's because we have been extremely respectful of our users' time. We fully plan to continue that." She said the company had no immediate plans to start telemarketing programs, but she added, "We intend to have maximum flexibility."

Ms. Nash said, however, that Yahoo's biggest objective in its new policy was to give it more freedom to sell its own services rather than those of its advertisers. Yahoo has been trying to recover from the slowdown in online advertising by introducing a raft of new fee-based offerings, like online games and expanded e-mail services.

Unlike other sites, Yahoo has never asked users specifically if they want to receive information about its own services. Rather, it has asked a single question authorizing it to send both messages for Yahoo services and messages for advertisers (which include Columbia House and the Discover Card, offered by a unit of Morgan Stanley Dean Witter (news/quote)).

Now Yahoo has sent tens of millions of users e-mail messages saying that it has given itself permission to send messages on behalf of its own services. Users have 60 days to go to a section of the site (subscribe .yahoo.com/showaccount) and reject such messages in 13 categories — one by one. The categories range from games to job hunting.

The distinction between messages from Yahoo and those from advertisers is not always clear because many companies do business under the Yahoo umbrella. Yahoo's travel channel, for example, is largely a Yahoo-brand version of the Travelocity (news/quote) online travel agent. Similarly, a message about back-to-school specials on Yahoo's shopping channel, for example, could well be paid advertising from some of the more than 10,000 stores in Yahoo's online mall.

"We believe in the products and services we offer," said Srinija Srinivasan, vice president and editor in chief at Yahoo. "Our network has grown so much we want to tell users about them."

Truste, a nonprofit group financed by Internet companies that creates standards for privacy policies, agreed to endorse Yahoo's move after an extended

discussion with the company. "I would not call what Yahoo did 'best practices,' " said Fran Maier, the group's executive director. "To the extent possible, you would like companies to honor the preferences that were previously set by the users. But on the other hand, we don't want to tell companies they can't do something when their business strategy changes. We have to balance those things."

Home | Back to Technology | Search | Help

Back to Top

Identity Theft Victim Stories
Privacy Rights Clearinghouse
www.privacyrights.org

[Submitted to the PRC May 2001]

The Credit Grantors Facilitated the Identity Theft Crime

My name is Kathleen Z. (not the actual name), and I am a victim of identity theft. Recently, my wallet (including credit cards, driver's license, passport, and social security number) was stolen from my office. Within an hour, my credit cards were being used to buy pagers, car audio equipment, cigarettes, liquor, etc.

Within two days, a woman was opening bank accounts, buying cell phones and commencing cell phone service, and applying for credit in my name. The last two months have been a nightmare.

However, I am extremely fortunate, in that my identity thief was arrested by the California Highway Patrol (following an unrelated traffic stop), and is currently being prosecuted in ABC County for a number of identity-theft related crimes. I am one of the lucky ones: My identity thief was caught carrying all of my identification (in addition to the identification of a number of other people). She was also carrying checks she had attempted to write on the fraudulent accounts, ATM/check cards for the fraudulent accounts, and several other pieces of information linking her to the theft of my identity. Most disturbingly, when she was arrested, and later while in custody, she continued to insist that her name was "Kathleen Z."

Despite the fact that my thief was arrested a week and a half ago, I am still fighting to clear my name, and I still dread opening my mailbox or answering the phone. Just a few days ago I discovered that my identity thief used my name, driver's license, and a fraudulent ATM/Visa check card issued in my name to pay for a hotel stay. (The issuer of the card had granted my thief a line of credit when she opened the fraudulent account, and persisted in honoring check card transactions despite a growing negative balance.) Just today I received another debt collection letter from Equifax Check Services, demanding payment of a bounced check written by my identity thief.

However, as stated above, I consider myself incredibly fortunate that, even if my identity thief only gets probation, she no longer has my identification in her possession. With two photo IDs and my social security number, this woman succeeded in completely disrupting my life, even though she looks nothing like me. I am only now beginning to put my life back together, although I am told that it will take years before I clear my credit reports of fraudulent inquiries and bounced check notices.

Just recently, I learned that there is a petty theft charge against me in the city of PQR, California, because my identity thief was caught shoplifting. My thief was not arrested at the time, but was instead issued a "ticket," in my name, with my driver's license number, my date of birth, but a different address. The police officer failed to notice that my thief misspelled my name when signing the ticket. If my thief had not been arrested later by the CHP, and if the PQR police had not run a check for my name in the course of executing a search warrant for a motel room the thief rented there in my name, I never would have learned that "I" have a date to appear in criminal court and answer to this charge, and a bench warrant would have been issued for me. (I still have not straightened all of this out, and as of now, I am still named as the defendant.)

In closing, I would like to add that one of the most disturbing aspects of all of this is that banks, credit card companies, and merchants facilitate identity theft through their policies and practices.

- Cingular One approved my identity thief's application for credit and cell phone service despite the fact that I had placed fraud alerts with all three major credit reporting agencies.
- Wells Fargo Bank permitted my identity thief to open an account in my name, using my photo IDs, and allowed her to withdraw $6,000 in cash, despite the fact that she had only deposited $100.
- Washington Mutual Bank also opened an account for her in my name, using my photo IDs, without running a credit check other than with ChexSystems. Despite a deposit of only $20, and a negative balance which eventually grew to over $4,000, Washington Mutual continued to honor my identity thief's transactions.
- ChexSystems only provides banks with information regarding misuse of bank accounts (e.g., overdrafts). They do not inform inquiring banks of recent requests by other banks, or of fraudulent activity. Nor is it possible to add a "fraud alert" to one's ChexSystems file. Consequently, when Washington Mutual Bank requested information about me, they were not told that Wells Fargo had requested information about me two weeks earlier.
- Several stores approved credit card transactions despite the fact that my thief either didn't sign the credit card slips, spelled my name wrong, or signed in a manner that did not look anything like my signature on the back of my credit cards.
- Still others allowed my thief to try credit card after credit card, until she found one that hadn't been reported stolen yet.
- Several other merchants accepted checks from my thief despite the fact that the spelling of my name in the signature did not match the spelling printed on the fraudulent checks.
- Numerous people accepted my photo ids without noting that this woman looks nothing like me, other than that we are both black and are both tall.

It's completely outrageous, and unacceptable.

Thank you for reading my e-mail to you, and for providing such excellent on-line resources.

Update: At a pre-trial hearing yesterday, the DA and my identity thief "resolved the case" with a plea bargain. She plead guilty to one of the 6 felonies with which she was charged. She will be sentenced in about a month, but will do no more than 6 months in County Jail. (I am told that she will most likely do 4 months.) She will then be on probation for 5 years. She will be ordered to pay restitution, and if she does so within 3 years, her probation will end then. All in all, the pre-trial hearing was very upsetting and disappointing, although I am not sure what I expected.

ELECTRONIC PRIVACY INFORMATION CENTER

Public Opinion on Privacy

Introduction | Privacy Polls and Studies | Resources

Introduction

Public opinion polls consistently find strong support among Americans for privacy rights in law to protect their personal information from government and commercial entities.

Individuals Should Be in Control of Both Initial Collection of Data and Data Sharing

The public considers opt-in--the principle that a company should obtain an individual's affirmative consent before collecting or sharing data--as one of the most important privacy rights. A March 2000 BusinessWeek/Harris Poll shows that 86% of users want a web site to obtain opt-in consent before even collecting users' names, address, phone number, or financial information. The same poll shows that 88% of users support opt-in as the standard before a web site shares personal information with others. An August 2000 Pew Internet & American Life Project Poll showed that 86% of respondents supported opt-in privacy policies. Historically, polls show similar support for the right to affirmative opt-in consent. For instance, a 1991 Time-CNN Poll indicated that 93% of respondents believed that companies should gain permission from the data subject before selling personal information.

Individuals Want Accountability and Security

Individuals report that they want the ability to obtain redress for privacy violations. An August 2000 Pew Internet & American Life report showed that 94% of Internet users thought that privacy violators should be disciplined. A February 2002 Harris Poll found that 84% of respondents thought it was important that access to data within an entity be limited.

Individuals Want Comprehensive Legislation, Not Self-Regulation

In numerous polls listed below, Americans report the current self-regulatory framework is insufficient to protect privacy. A February 2002 Harris Poll showed that 63% of respondents thought current law inadequate to protect privacy. A June 2001 Gallup poll indicated that two-thirds of respondents favored new federal legislation to protect privacy online. A March 2000 BusinessWeek/Harris Poll found that 57% of respondents favored laws that would regulate how personal information is used. In that same poll, only 15% supported self-regulation.

Individuals Value Anonymity

A series of surveys conducted by Georgia Institue of Technology's Graphic, Visualization, & Usability (GVU) Center repeatedly demonstrated strong support for Internet Anonymity. In the

GVU surveys, individuals expressed "strong agreement" with the statement that anonymity on the Internet is valuable.

Individuals Object to Web Tracking, Especially When Personal Information is Linked to the Profile

Web tracking for the purposes of building profiles is opposed by most individuals. A March 2000 BusinessWeek/Harris Poll found that 89% of respondents were uncomfortable with with web tracking schemes where data was combined with an individual's identity. The same poll found that 63% of respondents were uncomfortable with web tracking even where the clickstream data was not linked to personally-identifiable information. An August 2000 study conducted by the Pew Internet and American Life Project found that 54% of Internet users objected to tracking. A July 2000 USA Weekend Poll showed that 65% of respondents thought that tracking computer use was an invasion of privacy.

Individuals Do Not Trust Companies to Administer Personal Data and Fear Both Private-Sector and Government Abuses of Privacy

An April 2001 study conducted by the American Society of Newspaper Editors found that 51% of respondents were "very concerned" and 30% were "somewhat concerned" that a company might violate their personal privacy. 50% were "very concerned" and 30% were "somewhat" concerned that government might violate their personal privacy. The same study showed that 52% of respondents reported that they had "very little" or "no confidence at all" that private companies use personal information exactly the way they said they would. A February 2002 Harris Poll found that a majority of consumers do not trust businesses to handle their personal information properly.

Individuals Engage in Privacy Self-Defense

Since individuals realize that existing laws do not adequately protect their personal data, they often engage in privacy "self-defense." When polled on the issue, individuals regularly claim that they have withheld personal information, have given false information, or have requested that they be removed from marketing lists. In a February 2002 Harris Poll, 83% of respondents had asked a company to remove their name and address from mailing lists. An April 2001 study performed by the American Society of Newspaper Editors found that 70% of respondents had refused to give information to a company because it was too personal and 62% had asked to have their name removed from marketing lists.

Individuals Are Unaware of Prevalent Tracking Methods

Many Internet users cannot identify the most basic tracking tool on the Internet: the cookie. In an August 2000 study conducted by the Pew Internet and American Life Project, 56% of Internet users could not identify a cookie. It remains unknown whether individuals can identify more sophisticated tracking tools, such as "web bugs" or "spyware."

Notice

Users want notice of how their personal information is collected, used, and with whom it is

shared. In a March 2000 BusinessWeek/Harris Poll, 75% of respondents indicated that privacy notices were either "absolutely essential" or "very important."

Civil Liberties Post September 11th, 2001

Immediately after the September 11, 2001 terrorist attacks, polls showed that Americans were willing to accept more invasive police surveillance technologies such as facial recognition and greater collection of biometric identifiers. Additionally, many Americans reported greater trust in government, and that mere criticism of the government was inappropriate. As time passed, public support of these invasive technologies have waned. For instance, immediately after the attacks, a Harris Poll found that 68% of Americans supported a national ID system. A study conducted in November 2001 for the Washington Post found that only 44% of Americans supported national ID. A poll released in March 2002 by the Gartner Group found that 26% of Americans favored a national ID, and that 41% opposed the idea. Popular support for other surveillance technologies has declined as well.

Polls and Studies

The Attack on America and Civil Liberties Trade-Offs Survey (PDF), Institute for Public Policy and Social Research (IPPSR), Michigan State University, April 23, 2002. A Press Release and Slide Show are also available.

A telephone poll funded by the National Science Foundation of 1,448 adults nationwide between November 2001 and January 2002 found that:

92% reported that they opposed government investigation of non-violent protestors.

82% reported that they opposed government use of racial profiling.

77% reported that they opposed warrantless searches of suspected terrorists.

66% reported that they opposed monitoring of telephone and e-mail conversations.

55% reported that they were generally unwilling to allow the government broader powers to combat terrorism if those powers would limit traditional constitutional protections.

Privacy, Costs, and Consumers Privacy, Consumers, and Costs: How the Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete, (PDF Version) Robert Gellman, March 26, 2002.

In this report, Gellman identifies many behaviors that individuals engage in to protect personal information. These include, subscribing to called ID services, purchasing unlisted phone number, and entering false information at web sites. Gellman argues that "the costs incurred by both business and individuals due to incomplete or insufficient privacy protections reach tens of billions of dollars every year."

Atlanta Journal-Constitution Metro Atlanta Poll, March 2002. (Reported in What's for Sale? You. Atlantans Feel Victimized by Companies that Require Personal Data, Profit From It, Atlanta Journal Constitution, March 24, 2002, page 1A).

A poll of 2,400 adults in 15 metro Atlanta counties conducted by the Marketing Workshop found that:

65% reported that selling and buying personal information is an invasion of privacy.

43% reported that it is an invasion of privacy for stores to track purchasing habits.

Gartner Reports Strong Opposition to a U.S. National Identity Program, Gartner, March 12, 2002. (This poll is covered in Support for ID Cards Waning, Wired news, March 13, 2002.)

In a poll of 1,120 adults by Gartner, 26% of respondents reported that they were in favor of a national ID card, while 41% oppose the idea.

The poll demonstrated that respondents were suspicious of government agencies that would administer personal data, and that certain agencies, such as motor vehicle departments, were not trusted to run the system.

Americans maintain opposition to phone tapping, continue approval for random car searches, Zogby's Tracking Report, March 6, 2002.

In a survey of 1,011 registered American voters, Zogby's found that:

56% oppose allowing mail to be search at random.

74% oppose telephone conversations to be monitored.

51% favor allowing regular roadblocks to search vehicles.

E-Government Poll, Washington Post, February 27, 2002. (This poll appeared on the Washington Post Federal Page, and is not available online.)

A telephone poll of 961 adults conducted in November 2001 showed that Americans are sharply divided on the issue of national ID cards. 47% of respondents reported that national ID will improve interaction with government and business and 44% viewed it as "an invasion of people's civil liberties and privacy."

Privacy On and Off the Internet: What Consumers Want, Harris Interactive, February 19, 2002.

On behalf of Privacy & American Business, Ernst & Young, and the American Institute of Certified Public Accountants, Harris Interactive surveyed 1,529 adults and found the following:

Most consumers do not trust business to handle their personal information properly, and 84% responded that independent verification of company privacy policies should be a requirement.

Respondents reported concern for the following privacy risks: companies will sell data to others without permission (75%), transactions are not secure (70%), and crackers are able to steal personal data (69%).

83% reported that they would end business dealings with a company if the company misused customer information.

63% disagreed that existing law provides adequate protections against privacy invasions.

57% reported that most businesses do not handle personal information in a confidential and proper way.

In the offline context, 87% of respondents reported that they had refused to give information to a business because the collection of information was unnecessary or too personal. 83% had asked a company to remove their name and address from mailing lists.

The survey also illustrated that internal security of companies that collect personal data is important. For instance, 84% thought it was important that internal access to data be limited. 89% reported that companies should not release personal data without permission or legal justification.

Public Is Wary but Supportive on Rights Curbs, New York Times Poll, December 12, 2001.

A New York Times/CBS News Poll of 1,052 adult by phone found that:

65% reported being concerned about losing civil liberties.

75% reported that investigation of religious groups without cause violates rights.

65% of respondents reported that they did not want the government to monitor the communications of ordinary Americans to reduce the threat of terrorism.

Americans were divided on the increased use of wiretaps to deter terrorism. Immediately after the attacks, 53% supported more surveillance and 36% thought more surveillance would violate Constitutional rights. In December 48% supported more surveillance, and 44% though that surveillance would violate rights.

Overwhelming Public Support for Increasing Surveillance Powers and, Despite Concerns about Potential Abuse, Confidence that the Powers Will be Used Properly, Harris Poll, October 3, 2001.

A Harris Interactive poll of 1,012 adults by telephone finds that the public shows strong support for new surveillance technologies, but also that citizens are concerned about police abuse of new surveillance powers. 68% support national ID systems, and 86% support facial recognition technology.

However, respondents also expressed that these new surveillance technologies increased risk of police abuse. Respondents identified the following risks: profiling based on nationality, race, or religion (44% highly concerned), monitoring of innocent persons' communications (45% highly concerned), targeting of legitimate political groups (32% highly concerned).

Additionally, a majority of respondents reported that they were concerned that new police powers would be used for crimes other than terrorism and that judges would not give adequate oversight of police surveillance activities.

Online Privacy Continues to Be a Major Concern for Consumers, Yankee Group Trend Summary, August 2001. Cited in Yankee Group: 83% of Public Concerned About Privacy, EPIC Digest, August 8, 2001

A Yankee Group survey of 3000 online consumers found that 83% of respondents are somewhat or very concerned about privacy on the Internet.

Majority of E-mail Users Express Concern about Internet Privacy But only 28% are "very" concerned, Gallup Poll, June 28, 2001.

A Gallup Poll of e-mail users found that two-thirds of respondents favor federal legislation to ensure citizens' privacy online. Frequent users are more likely to favor the passage of new laws than infrequent users. Additionally, individuals under the age of 50 were among the strongest supporters of privacy laws.

Freedom of Information in the Digital Age, American Society of Newspaper Editors Freedom of Information Committee and the First Amendment Center, April 3, 2001. (Press release at Public support for government openness tempered by privacy concerns, Freedom Forum, April 3, 2001.)

In interviews with 1,005 adults, the American Society of Newspaper Editors (ASNE) and the First Amendment Center (FAC) found that:

89% were concerned about their personal privacy. Privacy, among the respondents, was as

important as concerns about crime, access to quality health care, and the future of the social security system.

54% agreed that laws should be strengthened to protect personal privacy, even if legislation resulted in losing access to some public records.

54% said that driver's license information "probably" or "should" not be made available to the public.

90% said that it was not legitimate for states to sell driver's license or car registration information to businesses.

60% "strongly approve" and 16% "somewhat approve" of the Driver's Privacy Protection Act, which requires opt-in consent before motor vehicle information can be released to businesses.

59% said that divorce records "probably" or "should" not be made available to the public.

76% either "somewhat" or "strongly" disagreed with the proposition that all government records should be made available over the Internet.

The ASNE/FAC study showed that individuals feared both commercial-sector and government invasions of privacy. 51% were "very concerned" and 30% were "somewhat concerned" that a company might violate their personal privacy. 50% were "very concerned" and 30% were "somewhat" concerned that government might violate their personal privacy.

19% were aware that a private company had misused their personal information.

7% were aware that the government had misused their personal information.

52% reported that they had "very little" or "no confidence at all" that private companies use personal information exactly the way they said they would.

40% reported that they had "very little" or "no confidence at all" that the government uses personal information exactly the way they said they would.

86% were concerned about private companies selling their personal information.

86% were concerned about the government selling their personal information.

70% had refused to give information to a company because it was too personal.

62% had asked to have their name removed from marketing lists.

71% believe that is acceptable for privacy laws to hinder marketers in their attempts to reach customers.

Surviving the Privacy Revolution, Forrester Research, March 2001. Press release at: Companies Must Adopt A Whole-View Approach To Privacy, Forrester Research, March 2001.

For this report, Forrester interviewed legal, academic, and industry experts, and application and content developers.

Forrester concluded that companies need to institutionalize respect for privacy in order to emerge as a credible organization.

The report also claims that 6% of Americans have a high level of trust in the storage of their personal information by web sites, and 7 out of 8 express interest in legislation protecting Internet privacy.

To Opt-In or Opt-Out? It Depends on the Question, Communications of the ACM, February 2001.

In this paper, researchers Steven Bellman, Eric Johnson, and Gerald Lohse argue that: "Using the right combination of question framing and default answer, an online organization can almost guarantee it will get the consent [for information collection] of nearly every visitor to its site."

Further, they found that "...if marketers wanted most people to say 'yes' to their privacy policy, all they have to do is make 'yes' the response recorded if a consumer takes no action."

They conclude: "Regulation that genuinely aims to promote consumer from privacy infringement should also stipulate the form of the question asking for a consumer's consent."

Privacy Concerns: Is It Time for the Government to Act?, Wirthlin Report, January 2001.

In telephone surveys of 1,201 adults in June 2000, 150 senior-level U.S. executives in September 2000, and a "quorum" survey of 1,000 adults in January 2001, Wirthlin Worldwide found that:

35% of consumers polled and 29% of corporate executives were "extremely worried or concerned" that their personal information might be misused by a company.

62% of consumers who did not shop online did not do so because of "major concerns" over privacy and security of their personal information.

The five most frequently mentioned feelings associated with transmitting personal information online were cautious (92%), hesitant (81%), suspicious (72%), uncertain (68%), and uneasy (64%).

Trust and Privacy Online: Why Americans Want to Rewrite the Rules, Pew Internet & American Life Project, August 20, 2000.

In a survey of 2,117 Americans, the Pew Internet & American Life Project found that:

86% support opt-in privacy policies before companies use personal information.

54% believe that web site tracking of users is harmful and privacy invasive.

24% of Internet users reported giving false information to a web site. 20% gave alternative or secondary e-mail addresses to web sites.

56% cannot identify a cookie.

The Pew study showed strong support for accountability. 94% of Internet users reported that privacy violators should be disciplined. This included support for prison terms (11%), fines (27%), and closing the offending website (26%).

The Internet and the Family 2000: The View from Parents, The View from Kids, University of Pennsylvania's Annenberg School for Communication, May 2000. (Press release at: The Internet and Family 2000, Annenberg Public Policy Center, May 16, 2000.)

This report analyzed the different attitudes of parents and kids towards giving out personal information online. Released in May 2000, the report found that children are more likely than their parents to reveal personal or family information online. Also, while 89% of parents believe that the Internet is beneficial, 74% of parents surveyed cited concerns about their children divulging personal information on the Web.

BusinessWeek/Harris Poll: A Growing Threat, BusinessWeek Magazine, March 2000.

A telephone poll of 1,014 adults conducted by Harris Interactive found that:

89% were uncomfortable with schemes that merged tracking of browsing habits with an individual's identity.

95% were uncomfortable with profiles that included tracking of browsing habits, identity, and other data, such as income and credit data.

57% favor laws to regulate how personal information is collected and used.

78% were concerned that businesses would use personal information to send unwanted junk mail.

63% were uncomfortable with tracking users' movements on the Internet, even when the clickstream was not linked to personally-identifiable information.

92% were uncomfortable with web sites that shared user information with other organizations.

93% were uncomfortable with web sites that sold user information to other organizations.

91% were uncomfortable with information sharing that allow tracking users across multiple web sites.

35% reported that privacy notices were "absolutely essential" and 40% reported that privacy notices were "very important."

56% reported that they would always "opt-out" of information collection if given the chance.

88% of respondents reported that web sites should gain affirmative opt-in consent before sharing personal information with others.

USA Weekend poll, USA Weekend Magazine, July 2, 2000.

In this poll, Opinion Research Group Corporation contacted a random sample of 1,017 adults in the United States between May 11-14, 2000. USA Weekend reported the following results:

43% say the government poses the greatest threat to their privacy

24% say the media pose the greatest threat

18% say corporations pose the greatest threat

84% say too many people have access to their credit report

79% say too many people have access to their financial records

62% say too many people have access to their driving record

61% say too many people have access to their medical records

75% of respondents report that phone calls at home from telemarketers are an invasion of privacy.

65% of respondents report that Internet companies tracking computer use is an invasion of privacy.

60% of respondents report that sending junk mail is an invasion of privacy.

47% of respondents report that receiving unsolicited e-mails from marketing companies is an invasion of privacy.

This study also demonstrated that many individuals engaged in privacy self-defense. 61% had

reported refusing to give out their credit card number, 58% refused to give out their Social Security number, 38% Limited the amount of information printed on checks, and 16% installed privacy software on their computers.

53% of respondents are extremely concerned with their ability to keep personal information private

51% of respondents think current laws do an inadequate job of protecting their right to privacy

---

The Internet's Privacy Migraine, Forrester Research, May 2000.

In this report, Forrester Researchers predict that consumer concern over privacy will result in two waves of privacy legislation in Congress. Congress should adopt technology-neutral privacy legislation, and self-regulatory efforts to education consumers will be likely to backfire.

Star Tribune Minnesota Poll, April 2000. (Reported in Minnesotans make public their desire for more privacy; Proposals to restrict telemarketers, others find broad support, Minnesota Star Tribune, April 6, 2000 at 1B.)

In a poll of 1,021 Minnesotans, the Star Tribune found that:

86% reported that they supported a state-administered do-not-call (DNC) list to avoid telemarketing sales calls.

87% reported that they supported a ban on the commercial sharing of their phone-calling and Web-browsing habits unless the company obtains a consumer's permission.

The IBM-Harris Multi-National Consumer Privacy Survey, Privacy & American Business, Vol. 7, No. 6, January 2000. This study is summarized online in IBM-Harris Survey Finds Privacy Active Consumers in Europe, U.S., PXNEWSFLASH, December 16, 1999.

More people in the United States believe that personal information is vulnerable to misuse than respondents in the United Kingdom or Germany.

Specifically, 94% of consumers surveyed in the United States think that personal information is vulnerable to misuse.
78% do so in the United Kingdom.
72% do so in Germany.

Consumers in all three countries also reported that they had refused to give information to a business for privacy reasons. Specifically, 78% of Americans, 58% of the British, and 52% of the German respondents reported withholding information.

Additionally, 58% of American respondents asked a company to remove them from marketing lists.

Wall Street Journal/NBC News Poll, Fall 1999. Reported in Report Slams Privacy Policies: Poll Finds Privacy is Top Concern, EPIC Alert, September 23, 1999.

A Wall Street Journal/NBC News poll of 2,025 adults by phone found that the loss of personal privacy was the number one concern of Americans as twenty-first century approaches. 29% of respondents reported that the "loss of personal privacy" was a top concern. Privacy outranked other high-profile concerns such as overpopulation (23%), terrorist acts (23%), racial tensions (17%), world war (16%), and global warming (14%).

The Privacy Best Practice, Forrester Research, September 1999. Press release at Forrester Technographics Finds Online Consumers Fearful Of Privacy Violations, Forrester Research, October 27, 1999.

A Forrester Research survey of 10,000 Americans and Canadians on consumer behavior found:

67% reported being extremely or very concerned about releasing personal information online.

54% of Internet users would not share their name with web sites.

90% report that they want the ability to control how their information is used after collection.

As a result of privacy risks online, Internet users spent $2.8 billion less online than they otherwise would have in 1999.

Beyond Concern: Understanding Net Users' Attitudes About Online Privacy, AT&T Research, April 14, 1999.

In a survey mailed to 1,500 individuals and completed by 381 people, AT&T researchers found:

Internet users are more likely to provide information when they are not identified.

Internet users dislike automatic data transfer.

AARP Survey, December 1998

The American Association of Retired Persons (AARP) conducted interviews with 501 randomly-selected AARP members.

78% of the respondents believed that federal and state laws are not strong enough to protect personal privacy from businesses that collect information about consumers.

92% objected to businesses selling their personal information.
93% objected to government selling their personal information.
87% objected to web sites selling their personal information.

81% opposed internal sharing of personal and financial information by businesses with their affiliates. 10% supported affiliate information sharing, however, a majority of that group specified that affiliate sharing should only occur after the institution gave notice and obtained written consent from the data subject.

A majority of respondents indicated that they wanted businesses to obtain individuals' consent before collecting information regarding bank account balances, medical history, product purchases, service purchases, long distance carrier information, Social Security Numbers, income, and financial assets owned.

42% of respondents did not know whom they would turn to for assistance if a company inappropriately shared or sold their personal information.

Graphic, Visualization, & Usability Center 10th WWW User Survey, October 1998.

A 1998 survey conducted by Georgia Institute of Technology's Graphic, Visualization, & Usability Center produced the following results:

26% of respondents had an unlisted phone number.

77% of respondents reported that privacy was more important than convenience.

Only 10% reported that an e-mail address should be collected when visiting a web page.

71% agreed with the statement that "there should be new laws to protect privacy on the Internet."

84% rejected the proposition that content providers have the right to sell user data.

90% agree that a "user ought to have complete control over which sites get what demographic information."

80% rejected the proposition that "Magazines to which I subscribe have the right to sell my name and address to companies they feel will interest me."

73% object to mass mailings that are specifically targeted to demographics.

90% objected to receiving "mass electronic mailings."

58% agreed that individuals "Ought to be able to Assume Different Aliases/Roles on the Internet."

93% agreed that "I ought to be able to communicate over the Internet without people being able to read the content."

52% agreed that "I would prefer Internet payment systems that are anonymous to those that are user identified."

82% objected to tracking individuals on the Internet for marketing purposes.

Graphic, Visualization, & Usability Center 8th WWW User Survey, October 1997.

A 1997 survey conducted by Georgia Institute of Technology's Graphic, Visualization, & Usability Center produced the following results:

25% of respondents did not know what "cookies" are.

72% agreed that new laws are needed to protect privacy on the Internet.

82% reject the notion that content providers have the right to resell user information.

Money Magazine Poll, August 1997.

88% of the public favors a privacy bill of rights. This bill of rights would require companies to tell consumers and employees exactly what kind of personal information they collect and how they use it.

Graphic, Visualization, & Usability Center 7th WWW User Survey, April 1997.

A 1997 survey conducted by Georgia Institute of Technology's Graphic, Visualization, & Usability Center produced the following results:

Approximately 40% of respondents reported that they had provided false information to web sites. 14% of respondents reported falsifying information over 25% of the time that they provided personal data.

As with the 1996 study, the 7th WWW study also found strong support for anonymity. When asked to rate certain issues on a 1 to 5 scale with 5 representing "strong agreement," respondents supported private communication on the Internet (4.70), respondents supported the anonymous nature of the Internet (4.46), respondents favored new laws to protect Internet privacy (3.79), respondents favored anonymous payment systems (3.93), and respondents favored the ability to create multiple aliases on the Internet (3.67).

Graphic, Visualization, & Usability Center 6th WWW User Survey, October 1996.

A 1996 survey conducted by Georgia Institute of Technology's Graphic, Visualization, & Usability Center produced the following results:

33% of respondents reported providing false information to a web site while registering.

The study found strong support for anonymity. When asked to rate certain issues on a 1 to 5 scale with 5 representing "strong agreement," respondents supported private communication on the Internet (4.70), respondents supported the anonymous nature of the Internet (4.46), respondents favored new laws to protect Internet privacy (3.79), respondents favored anonymous payment systems (3.93), and respondents favored the ability to create multiple aliases on the Internet (3.67).

Direct Magazine, June 15, 1996.

86% reported that they supported legislation that would establish an opt-in procedure before names were included on a mailing list.

78% reported that they supported an opt-in system, even if it meant that they would not receive new mailings.

58% reported that they wanted to outlaw the collection and dissemination of Social Security numbers.

A copy of the full report can be ordered from DIRECT Survey, Cowles Business Media, 470 Park Ave. South, New York, NY 10016.

Graphic, Visualization, & Usability Center 5th WWW User Survey, May 1996.

A 1996 survey conducted by Georgia Institute of Technology's Graphic, Visualization, & Usability Center produced the following results:

When asked to rate certain issues on a 1 to 5 scale with 5 representing "agree strongly ," respondents supported anonymity on the Internet (4.6), they supported "complete" control over demographic information (4.4), and they support the ability to assume different aliases on the Internet (3.7).

Internet users strongly disagreed with the proposition that content providers have the right to resell users' information (1.7).

Attitudes Towards Wiretapping, Roper Center for Public Opinion Research, Published in the 1994 Bureau of Justice Statistics Sourcebook of Criminal Justice Statistics.

Since 1974, between 70-80% of respondents report that they oppose wiretapping.

1991 TIME-CNN Poll

93% of respondents believed that the law should require companies to obtain permission from consumers before selling their personal information.

1990 Harris Poll

79% of respondents believed that the drafters of the Declaration of Independence would have included "privacy" along with the rights of "life, liberty, and the pursuit of happiness."

Resources

- Privacy, Costs, and Consumers Privacy, Consumers, and Costs: How the Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete, Robert Gellman, March 2002.
- Oscar H. Gandy, Jr. *The role of theory in the policy process. A response to Professor Westin.* pp. 99-106 in C. Firestone and J. Schement (Eds.). Toward an Information Bill of Rights and Responsibilities. Washington DC: The Aspen Institute Communications and Society Program, 1995.
- Privacy Rights Clearinghouse Poll Page.
- About Polling, Public Agenda.org.
- 20 Questions Journalists Should Ask About Poll Results, National Council on Public Polls.
- Best Practices for Survey and Public Opinion Research, American Association of Public Opinion Research.

EPIC Privacy Page | EPIC Home Page

Last Updated: April 25, 2002
Page URL: http://www.epic.org/privacy/survey/default.html

Getting a Handle on Privacy's Fine Print

Financial Firms' Policy Notices Aren't Always 'Clear and Conspicuous,' as Law Requires

By Robert O'Harrow Jr.
Washington Post Staff Writer
Sunday, June 17, 2001; Page H01

For today's financial services quiz, dear readers, you will be asked to determine the meaning of the following passages. They're taken from privacy notices recently sent to customers by banks, securities firms and insurance companies.

"If you prefer that we not disclose nonpublic personal information about you to nonaffiliated third parties, you may opt out of those disclosures, that is, you may direct us not to make those disclosures (other than disclosures permitted by law)."

"If you choose not to receive such solicitations from unaffiliated third parties, you may instruct [the bank] not to disclose your non-public personal information."

"An affiliate is a company we own or control, a company that owns or controls us, or a company that is owned or controlled by the same company that owns or controls us. Ownerships does not mean complete ownership, but means owning enough to have control."

If you don't get it all, don't feel too bad. A lot of other people are having the same trouble.

"Unless you're a lawyer, you're going to have a hard time

Consumer Corner

Minimize exposure to fraud artists:

- Don't give out personal information to others without asking how it will be used.
- Make sure there's a compelling reason before providing someone with your Social Security number.
- Pay attention to credit card bills and bank statements. If there are unfamiliar charges, or if the bills do not arrive on time, quickly call the company involved.
- Pick up mail promptly. Shred personal documents and mail, or remove personally identifiable information before disposing of it.
- Review your credit report periodically for unusual listings.

Read More:

- Avoid Becoming a Victim of Identity Theft (pdf)
Source: Office of the Comptroller

- ID Theft: When Bad Things Happen to Your Good Name (pdf)
Source: FDIC

On Washtech.com

- Night and Day, Computers Collect Information
- **Grapic:** Life of the Data Dealers
- More in Washtech.com

On the Web

- OCC Press Release: Identity Theft Increasing
- OCC Advisory Letter to Banks on Identity Theft and Pretext Calling
- Comptroller of the Currency, Administrator of National Banks
- FDIC Guidance on Identity Theft and Pretext Calling
- Federal Deposit Insurance Corporation

understanding this," said Mark Hochhauser, a readability consultant in Minnesota who recently reviewed more than 30 such notices for a privacy group. "Having a PhD is no guarantee that you can understand these things."

A billion or more of the privacy policies are being mailed out this spring – more than 10 per household on average – under the requirements of the historic 1999 banking deregulation law. Companies have until July 1 to tell customers in a "clear and conspicuous" style, according to the rule, how information about them is gathered and used.

Consumers are supposed to be told they can ask banks to withhold information about their accounts and transactions from third-party companies. They also have the right to "opt out" – using toll-free numbers or letters – of sharing credit information. At the same time, many companies note that consumers can't prevent the flow of personal data among affiliates.

——Web Special——
• Privacy

——Related Articles——
• Gov't Credit Card Fraud Info Unknown (Associated Press, May 1, 2002)
• Export-Import Bank Operations Extended (Associated Press, May 1, 2002)
• House OKs Export-Import Bank Plan (Associated Press, May 1, 2002)
• More Financial Services News

E-Mail This Article
Printer-Friendly Version
Subscribe to The Post

Industry leaders insist customers are reading the notices. American Bankers Association officials estimate that fewer than 5 percent of the people receiving notices so far are choosing to "opt out."

But association spokeswoman Catherin Pulley acknowledged that many people might be simply tossing the documents in the trash. "We know that consumers don't read their mail," she said. "It is a cause of concern. We're worried about it."

So are some consumer advocates-cum-English teachers, who have taken to chiding bankers about their use of the language.

"They're unintelligible, we believe – almost purposefully so," said Edmund Mierzwinski, consumer program director for the U.S. Public Interest Research Group. Mierzwinski said he believes that companies are intentionally playing down consumers' right to say no to information-sharing.

Beth Givens, director of the Privacy Rights Clearinghouse, a nonprofit group in San Diego, said dozens of people have contacted her group for advice on how to read the policies. "They think their banks are trying to hoodwink them," she said.

Banking officials bristle at the criticism. John Byrne, senior counsel at the bankers association, denied the notices were intended to confuse and said members stand ready to help explain their policies to customers.

"What is really frustrating to us is the spin some consumer groups are putting on this," he said. "It's offensive to us. Everybody has worked very hard on this."

Despite the effort, language specialist Hochhauser said companies repeatedly use too many words in each sentence and too many uncommon words.

People would need to read at the level of a third- or fourth-year college student to properly understand the nuances of most of the privacy statements, he said, while most people read at a junior-high-school level.

Hochhauser said, "People have a very hard time figuring out what you mean when you use two or three or four negatives in a sentence," he said. "It just confuses things immensely."

His analysis, which uses computer software programs, rates Marquette Bank's policy as one of the the most difficult to read. It's nine pages long and includes passages such as this:

"If you are a consumer and don't want us to share your nonpublic personal information, other than Experience Information, with our Affiliates for any purpose, then you may 'opt out' by completing the Consumer Opt Out form."

Kathleen W. Collins, a lawyer who specializes in banking law, generally praised the industry's effort. She said that banks and other institutions probably erred by hewing too closely to the actual language of the regulations.

"The time and money which have gone into complying with this law and regulations is extraordinary," she said. "Banks don't want to get creative over privacy – they want to comply with the law, keep their customers happy and not get criticized by the regulator or sued by the state attorney general. Tracking the language found in bank regulations has traditionally created a safe harbor from lawsuits, so that is what most banks did."

For further information about the privacy notice issue, visit the Web sites of the Privacy Rights Clearinghouse,

www.

privacyrights.

org

, which includes a sample "opt out" letter, or the American Bankers Association,

www.

aba.

com

Related Links

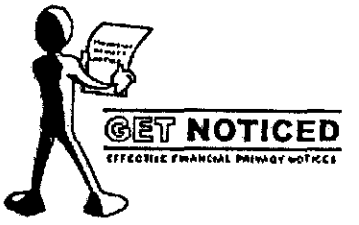
Latest Business News
Manufacturing Grows for 3rd Straight Month (Reuters, 5/1/02)
States Pressing Analyst Probe (The Washington Post, 5/1/02)

Federal Screeners Take Up Posts at BWI Checkpoints (The Washington Post, 5/1/02)

Full Business Section

Full Washtech Section

Interagency Public Workshop: Get Noticed: Effective Financial Privacy Notices December 4, 2001



If you were unable to attend, you can access information through this site, including audio, CD-Rom and transcripts of the workshop.

The Gramm-Leach-Bliley Act (GLB Act) requires that financial institutions issue privacy notices to their customers, and, in certain circumstances, provide them with the opportunity to opt out of disclosures of nonpublic personal information to nonaffiliated third parties. Concerns have been raised about the clarity and effectiveness of some of the privacy notices. At the same time, some financial institutions have sought additional guidance about the form and content of their notices from the federal agencies charged with implementing and enforcing the GLB Act.

To address these critical and timely issues, the eight federal agencies (GLB Agencies) that issued regulations implementing the Act's privacy provisions will held a joint public workshop, entitled Get Noticed: Effective Financial Privacy Notices, on Tuesday, December 4, 2001. The workshop addressed the challenges of and strategies for providing effective notice under the GLB Act. This interagency effort brought together government officials, financial institutions, industry associations, consumer and privacy advocates, and communications experts to discuss these issues through moderated panel discussions.

The GLB Agencies are:

- Board of Governors of the Federal Reserve System
- Commodity Futures Trading Commission
- Department of Treasury, Office of the Comptroller of the Currency
- Department of Treasury, Office of Thrift Supervision
- Federal Deposit Insurance Corporation
- Federal Trade Commission
- National Credit Union Administration
- Securities and Exchange Commission

The Get Noticed presentations, biographies, publications and other resources are available on a CDRom from the FTC. For a free copy, send email to glbworkshop@ftc.gov with your name, address, and telephone number and the subject "GLB CDRom Request."

- **Workshop Transcripts** [PDF ONLY - 409K]
- **Public Comments**
- **Conference Presentations & Supporting Documents** [Please note file sizes]

The Challenges of Providing Effective Financial Privacy Notices: The Consumer and Academic Perspective		
Mary Culnan, *Bentley College* **Consumers & Privacy Notices**	[PDF]	[PPS] 103K
The Culnan-Milne Survey on Consumers & Online Privacy Notices: Summary of Responses Mary J. Culnan & George R. Milne	[PDF]	
E. Joyce Gould, *Citizen Action of New York* **Your Privacy is Important to Us?**	[PDF]	[PPS] 64K
Consumers' Privacy Concerns, *Citizen Action of New York*	[PDF]	